

ARIS RISK & COMPLIANCE MANAGER
ADMINISTRATIONS-
HANDBUCH

VERSION 10.0 - SERVICE RELEASE 16
OKTOBER 2021

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 - 2021 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 <https://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 <https://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 <https://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Inhalt

1	Einleitung	1
2	Administration	2
2.1	Konfiguration des Event-Enabling in ARIS Risk & Compliance Manager.....	2
2.2	Modellierte Benutzer übertragen.....	5
2.2.1	Modellierte Benutzer exportieren	5
2.2.2	Modellierte Benutzer ins User Management importieren	6
2.2.3	Benutzer mit ARIS Administration/User Management synchronisieren.....	8
2.3	Anbindung an einen Verzeichnisdienst (LDAP)	9
2.4	Anbindung an ARIS Publisher.....	10
2.5	Runnable über ARIS Cloud Controller sichern und rücksichern.....	13
2.6	Runnable über ARIS Tenant Management sichern und rücksichern.....	13
2.7	ARCM mit anderen Mandanten als dem 'Standard'-Mandanten verwenden.....	13
2.8	Sprachen in ARIS Administration wählen.....	14
2.9	Anpassen der Zeitplanung.....	15
3	Glossar.....	18
4	Rechtliche Hinweise.....	19
4.1	Dokumentationsumfang.....	19
5	Index.....	i

1 Einleitung

ARIS Risk & Compliance Manager ist eine Web-Anwendung. ARIS Risk & Compliance Manager verwendet Java-Servlets und Java-Server-Pages (JSP), die neben einer Java-Umgebung (JDK) einen Web-Container, d. h. Servlet-Container (Apache-TomEE) als Ablaufumgebung benötigen. Die Daten werden in einem relationalen Datenbanksystem gehalten und durch eine JDBC-Schnittstelle mit der Anwendung ausgetauscht. Zu Testzwecken oder für kleine Umgebungen (bis zu 50 gleichzeitige Benutzer) können Sie ARIS Risk & Compliance Manager mit der Datenbank **PostgreSQL** verwenden. Für den Produktivbetrieb benötigen Sie das Datenbanksystem **Oracle** oder **Microsoft®-SQL-Server**.

2 Administration

2.1 Konfiguration des Event-Enabling in ARIS Risk & Compliance Manager

ARIS Risk & Compliance Manager bietet die Möglichkeit, Events von einem Messaging-Provider (Standard: Universal-Messaging digitaler Ereignisservices) zu abonnieren und daraus in ARIS Risk & Compliance Manager definierte Objekte zu generieren, z. B. Kontrolltests. Die Steuerung durch Events wird während des Setups oder nachträglich über ARIS Cloud Controller konfiguriert. Sie erhalten Informationen zu Vorgehen sowie Hintergrundinformationen in der Online-Hilfe unter **Was ist Event-Enabling?** oder im Videotutorial **Event-Enabling**.

Beispiele - Befehle für 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:/EventsRoutingConfigurat
ion
reconfigure arcm_m
arcm.config.eventProviderServiceAlias="UniversalMessaging"
reconfigure arcm_m arcm.config.useDurableEventSubscriptions="true"
```

BEDEUTUNG DER PARAMETER

- **arcm.config.eventProviderActive**
Zentrale Angabe zur Aktivierung des Event-Enabling. Ist der Wert **false** angegeben, wird der Service nicht gestartet. Bei **true** müssen die weiteren Parameter des **Event-Enabling** gültige Werte enthalten.
- **arcm.config.eventProviderUrl**
Der Parameter muss die gültige URL einer Universal-Messaging-Server-Instanz enthalten, z. B. **nsp://eventserver:9000**.
- **arcm.config.eventProviderServiceAlias**
Die Kennung des Services bzw. der zu verwendenden Nachrichteneinstellungen. Standard ist **UniversalMessaging**.
- **arcm.config.eventSagInstallationLocation**
Gibt den absoluten Pfad zum Wurzelverzeichnis einer lokalen SAG-Installation oder zum Wurzelverzeichnis des extrahierten Nicht-OSGi-Client-Archivs an. Beispiel:
C:\SoftwareAG
- **arcm.config.eventRoutingConfigurationLocation**

Gibt den absoluten Pfad zu einem beliebigen Verzeichnis an, an dem die Routing-Konfiguration gespeichert ist. Beim ersten Starten der Anwendung wird automatisch das Unterverzeichnis **DigitalEventServices** angelegt, um die Out-of-the-box-Konfiguration zu speichern. Beispiel: **C:\EventsRoutingConfiguration**

- **arcm.config.useDurableEventSubscriptions**

Standardmäßig arbeitet das Event-Enabling mit dauerhaften Abonnements von Messages. Diese Funktionalität kann deaktiviert werden, indem dieser optionale Parameter auf den Wert **false** gesetzt wird.

DIGITALE EREIGNISTYPEN UNTERSTÜTZEN

Um aus den in ARIS Risk & Compliance Manager empfangenen Ereignissen definierte Objekte zu generieren, werden vordefinierte digitale Ereignistypen mitgeliefert. Beim ersten Starten der Anwendung werden die unter dem Namensraum **des.aris.arcm** gebündelten, spezifischen digitalen Ereignistypen automatisch im Standardspeicherort der **Event-Typen** der SAG-Installation angelegt. Beispiel:

C:/SoftwareAG/common/DigitalEventServices/TypeRepository/eventtypes/des/aris/arcm

Diese müssen in das TypeRepository des Event-generierenden Systems kopiert werden. Das Verschicken von Events mithilfe der in ARIS Risk & Compliance Manager mitgelieferten digitalen Ereignistypen ist Bestandteil von Complex Event Processing. Weitere Informationen hierzu entnehmen Sie bitte der Dokumentation von Complex Event Processing.

BETRIEB EINER AUTARKEN INSTALLATION VON ARIS RISK & COMPLIANCE MANAGER

Liegen ARIS Risk & Compliance Manager und Universal-Messaging-Server nicht auf dem gleichen Host, können die benötigten Konfigurationen und Ressourcen nicht direkt referenziert und verwendet werden. In diesem Fall können die Ressourcen mit dem Tool **NonOsgiClientArchiveCreator**, das im Ordner **Add-ons/UniversalMessaging/ARCM** des ARIS Risk & Compliance Manager-Installationsmediums zur Verfügung steht, aus der SAG-Installation extrahiert werden. **NonOsgiClientArchiveCreator.zip** muss in das Host-System der SAG-Installation entpackt werden, anschließend kann **createClientArchive** (Batch-Skript oder Shell-Skript) ausgeführt werden. Beide Skripte benötigen eine vorhandene Java-Laufzeitinstallation auf dem Host-System. Bei einem Linux-System müssen möglicherweise die Berechtigungen für den Wurzelordner des entpackten Tools geändert werden, z. B. `sudo chmod -R 777 ./`. Das Skript **creatClientArchive** fragt den Pfad der lokalen SAG-Installation ab und extrahiert dann alle erforderlichen Ressourcen, einschließlich der Lizenzinformationen, in das Archiv **./build/UniversalMessagingNonOsgiClient.zip**. Das Archiv **UniversalMessagingNonOsgiClient.zip** muss anschließend in das Host-System der ARIS Risk & Compliance Manager-Installation entpackt und referenziert werden, wie bereits für den Konfigurationsparameter **arcm.config.eventSagInstallationLocation** beschrieben.

*Weiterführende Information zum Betrieb von Universal-Messaging, insbesondere die Konfiguration durch den Software AG Platform-Manager, entnehmen Sie bitte den produktspezifischen Dokumentationen.

Warnung

Um den fehlerfreien Betrieb und die Kompatibilität zu gewährleisten, achten Sie bitte darauf, die Version der kopierten Ressourcen der Installation von ARIS Risk & Compliance Manager immer mit der Version des verwendeten Universal-Messaging-Servers synchron zu halten.

2.2 Modellierte Benutzer übertragen

2.2.1 Modellierte Benutzer exportieren

Bei der Übertragung von Risk & Compliance-Daten von ARIS nach ARIS Risk & Compliance Manager werden die modellierten Benutzer nicht von ARIS Architect nach ARIS Administration/User Management übertragen. Sie können stattdessen die modellierten Benutzer mit dem Report **ARCM-Benutzerexport für User Management** aus ARIS Architect exportieren und die Benutzer mit der Datei **create_user.bat** nach ARIS Administration/User Management importieren. Anschließend synchronisieren (Seite 8) Sie die Benutzer in ARIS Risk & Compliance Manager mit Benutzern in ARIS Administration/User Management, um die Benutzerkonten in ARIS Risk & Compliance Manager zu übertragen. Detaillierte Informationen zum Benutzer-Management in ARIS Administration/User Management finden Sie in der **ARIS Administration**-Hilfe in ARIS Connect oder in der **User Management**-Hilfe. Detaillierte Informationen zu Export, Import und Synchronisation von Benutzern finden Sie im **ARCM - Administrationshandbuch** im Kapitel **Administration > Modellierte Benutzer übertragen**. Beachten Sie, dass in ARIS Architect modellierte Benutzer nicht automatisch in ARIS Risk & Compliance Manager verfügbar sind.

Dieses Vorgehen ist nur für Produktschulungen und -vorstellungen relevant. Bei Produktivsystemen erfolgt die Verwaltung der Benutzer für alle ARIS-Produkte zentral in ARIS Administration/User Management (ARIS Connect).

Folgende Attribute eines Benutzers werden exportiert: Anmeldung, Vorname, Nachname und E-Mail-Adresse. Der Report ermittelt außerdem, welches Lizenzrecht ein Benutzer benötigt. Dabei gelten folgende Regeln:

- Ist ein Benutzer keiner Benutzergruppe zugeordnet, wird ihm das Lizenzrecht **Contribute** zugeordnet. Benutzer ohne Gruppenzuordnung sind berechtigt, Aufgaben im Issue-Management wahrzunehmen.
- Ist ein Benutzer einer Benutzergruppe mit der Rolle Vorfall-Owner oder Policy-Addressee zugeordnet, wird ihm das Lizenzrecht **Contribute** zugeordnet.
- Bei allen anderen Rollenzuordnungen erhält der Benutzer das Lizenzrecht **Operate**.

Voraussetzungen

- Sie benötigen das Zugriffsrecht **Lesen** für die Gruppen, in denen die Datenbankelemente gespeichert werden.
- Die Elemente wurden gespeichert.
- Sie können auf dieses Skript zugreifen. Der Zugriff auf Skripte kann auf bestimmte Benutzergruppen beschränkt sein.

Vorgehen

1. Starten Sie ARIS Architect.
2. Klicken Sie auf **ARIS** >  **Explorer**. Die Registerkarte **Explorer** wird geöffnet.
3. Klicken Sie in der Leistenanzeige auf  **Navigation**, wenn die Leiste **Navigation** noch nicht aktiviert ist.
4. Öffnen Sie die Datenbank, deren modellierte Benutzer Sie exportieren möchten.
5. Klicken Sie mit der rechten Maustaste auf die Hauptgruppe.
6. Klicken Sie auf **Auswerten** > **Report starten**.
7. Wählen Sie die Kategorie von **ARIS Risk & Compliance Manager**.
8. Wählen Sie den Report **ARCM-Benutzerexport für das User Management**.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie die Ausgabeinstellungen.
11. Klicken Sie auf **Fertigstellen**.

Eine Textdatei mit den Attributen Anmeldung, Vorname, Nachname sowie E-Mail-Adresse wird exportiert. Es werden die Benutzer angezeigt, die wegen fehlender Attribute vom Export ausgeschlossen wurden. Sie haben so die Möglichkeit, die benötigten Attribute einzutragen und durch erneutes Starten des Reports alle Benutzer zu exportieren.

Importieren (Seite 6) Sie nun die Benutzer mit der Datei **create_user.bat** in ARIS Administration/User Management.

2.2.2 Modellierte Benutzer ins User Management importieren

Importieren Sie die modellierten Benutzer ins User Management.

Vorgehen

1. Legen Sie das Installationsmedium von ARIS Risk & Compliance Manager in das Laufwerk.
2. Kopieren Sie die Datei **create_user.bat** aus dem Ordner **Content** in den Ordner **<ARCM-Installationsordner>\server\bin\work\work_umcadmin_s\tools\bin**.
3. Kopieren Sie die Textdatei, die Sie zuvor mit dem Report **ARCM-Benutzerexport für das User Management** erstellt haben, in den gleichen Ordner.
4. Ersetzen Sie in der Datei **create_user.bat** den Eintrag **set INPUTFILE** mit dem entsprechenden Namen der Exportdatei.
5. Speichern Sie die Änderung.
6. Führen Sie die Datei **create_user.bat** aus. Sie können dabei ein Kennwort für alle importierten Benutzer vergeben. Möchten Sie kein Kennwort vergeben, drücken Sie die **Eingabetaste**, ohne ein Kennwort einzugeben.

Die Benutzer werden ins User Management importiert.

Anschließend synchronisieren (Seite 8) Sie die Benutzer in ARIS Risk & Compliance Manager mit Benutzern in ARIS Administration/User Management.

2.2.3 Benutzer mit ARIS Administration/User Management synchronisieren


Sie können Benutzer in ARIS Risk & Compliance Manager mit Benutzern in ARIS Administration/User Management synchronisieren, um die Daten in ARIS Risk & Compliance Manager zu aktualisieren. Detaillierte Informationen finden Sie unter **Wo werden die Benutzer verwaltet?**.

Voraussetzung

Sie haben die Rolle **Systemadministrator** oder **Benutzer-/Benutzergruppenadministrator** mit Rollenlevel **umgebungsübergreifend**.

Vorgehen

1. Klicken Sie auf  **Administration > User Management**.
2. Klicken Sie unter **User Management > Mit User Management synchronisieren** auf **Synchronisieren**. Die Benutzerdaten in ARIS Risk & Compliance Manager werden durch die Daten aus ARIS Administration/User Management ersetzt. Dadurch werden Funktions- und Lizenzrechte, Namen, Kennwörter, E-Mail-Adressen usw. aktualisiert sowie Benutzer aktiviert.

Der Dialog wird geschlossen.  **Administration > Monitoring > Funktional > Server-Aufträge** wird angezeigt. Der Server-Task wird unter **Server-Tasks in Bearbeitung** ausgegeben. Wenn er abgeschlossen ist, wird er unter **Abgeschlossene Server-Aufträge (letzte 10)** aufgelistet.

2.3 Anbindung an einen Verzeichnisdienst (LDAP)

Anders als in den Vorgängerversionen wird LDAP nun nicht mehr direkt mit ARIS Risk & Compliance Manager verbunden. Stattdessen muss die LDAP-Anbindung in ARIS Administration/im User Management konfiguriert werden. Detaillierte Informationen hierzu finden Sie im Handbuch **ARIS SSO, LDAP, KERBEROS, SAML, SCIM** im Kapitel **Use LDAP**.

2.4 Anbindung an ARIS Publisher

Sie können eine Verbindung von ARIS Risk & Compliance Manager zu ARIS Publisher herstellen, um Objekte und Modelle aus ARIS Publisher in ARIS Risk & Compliance Manager anzuzeigen. Gemäß dem empfohlenen Vorgehen sollten die Stammdaten (Benutzer, Risiken, Kontrollen, usw.) in ARIS Architect modelliert werden. Nach der Modellierung können diese Daten mit dem Export-Report aus ARIS exportiert und in ARIS Risk & Compliance Manager importiert werden. Zusätzlich ist es möglich die Datenbank von ARIS Architect mit ARIS Publisher zu veröffentlichen. Nach dem Import der Stammdaten in ARIS Risk & Compliance Manager kann über die Umgebungen die Anbindung an ARIS Publisher konfiguriert werden. Dadurch kann z. B. in ARIS Risk & Compliance Manager von einem Risikoformular auf das Objekt im veröffentlichten Modell verlinkt werden, um den Prozess in ARIS Publisher anzuzeigen.

Voraussetzung


ARIS Risk & Compliance Manager und ARIS Publisher verwenden das gleiche ARIS Administration/User Management zur Verwaltung von Benutzern.

Vorgehen

USER MANAGEMENT

1. Starten Sie das User Management.
2. Legen Sie im User Management eine Benutzergruppe und einen Benutzer an.
3. Ordnen Sie dem Benutzer diese Benutzergruppe zu.
4. Ordnen Sie der Benutzergruppe das Funktionsrecht **Publisher-Administrator** zu.

ARIS ARCHITECT

1. Starten Sie ARIS Architect.
2. Klicken Sie auf **ARIS** >  **Administration**. Die Registerkarte **Administration** wird geöffnet.
3. Melden Sie sich an der Datenbank an, die Sie exportieren möchten.
4. Klicken Sie in der Navigation auf **Benutzer**. Die Benutzer und Benutzergruppen werden angezeigt.
5. Klicken Sie mit der rechten Maustaste auf die zuvor erstellte Benutzergruppe.
6. Klicken Sie auf **Eigenschaften**.
7. Klicken Sie auf **Funktionsrechte**.
8. Aktivieren Sie das Kontrollkästchen für das Recht **Datenbankexport**. (Die produktspezifischen Berechtigungen werden nicht zentral im User Management zugewiesen, sondern im jeweiligen ARIS-Produkt.)

9. Klicken Sie auf **Zugriffsrechte**.
10. Ordnen Sie der Benutzergruppe mindestens das Zugriffsrecht **Lesen** für die Hauptgruppe zu.
11. Klicken Sie auf **Rechte vererben**, um die Rechte auf alle Untergruppen zu übertragen.
12. Klicken Sie auf **OK**.
13. Veröffentlichen Sie die gewünschte Datenbank.
14. Ändern sie nach dem Export den Status auf **Aktiviert**.


ARIS PUBLISHER

1. Starten Sie ARIS Architect.
2. Melden Sie sich mit dem Benutzer **root** und dem Kennwort **root** an.
3. Öffnen Sie das Modul **Gruppen**. Die von Ihnen angelegte Benutzergruppe wird angezeigt.
4. Klicken Sie in der Zeile der Gruppe auf **Zuordnen**. Der entsprechende Dialog wird geöffnet.
5. Ordnen Sie die zuvor im User Management angelegt Gruppe ARIS Publisher zu.
6. Klicken Sie auf **Speichern**.

ARIS PUBLISHER-INTEGRATION IN ARIS RISK & COMPLIANCE MANAGER AKTIVIEREN


Voraussetzung

Sie haben die Rolle **Systemadministrator**.

1. Starten Sie ARIS Risk & Compliance Manager.
2. Klicken Sie auf  **Administration**. Das Menüelement **Allgemein** wird anfänglich angezeigt.
3. Klicken Sie unter **Umgebungsmanagement** auf **Umgebungen**.
4. Klicken Sie auf den Namen der gewünschten Umgebung. Das Formular wird angezeigt.
5. Klicken Sie unter **Einstellungen für die Integration von ARIS Publisher > ARIS Publisher-Integration** auf **Ja**.
6. Tragen Sie im Feld **Objektverknüpfung** den ARIS Publisher-Link in folgender Form ein:
http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<Benutzername>&password=<Kennwort>&localeid=1033&ph=<exportID>&objectguid={GUID}
7. Ersetzen Sie die Platzhalter folgendermaßen:
 - a. **<BusinessPublisherServer>** = Name oder IP-Adresse des ARIS Publisher Servers.
 - b. **<Benutzername>** = Name des Benutzers, der zuvor angelegt wurde.
 - c. **<Kennwort>** = Kennwort des Benutzers, der zuvor angelegt wurde.
 - d. **<exportID>**
 1. Öffnen Sie ein Modell in ARIS Publisher.

2. Klicken Sie mit der rechten Maustaste auf ein Objekt.
3. Klicken Sie auf **Link kopieren**.
4. Kopieren Sie im angezeigten Link den Parameter **ph** mit seinem Wert und ersetzen Sie damit **<exportID>**.

Der Platzhalter **{GUID}** muss nicht ersetzt werden. Dieser wird von ARIS Risk & Compliance Manager dynamisch ersetzt.

8. Tragen Sie in das Feld **Modellverknüpfung** den zuvor angelegten Link in der folgenden Form ein und ersetzen Sie den Parameter **objectguid** durch **modelguid**:
http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<Benutzername>&password=<Kennwort>localeid=1033&ph=<exportID>&modelguid={GUID}
9. Ersetzen Sie die Platzhalter.
10. Klicken Sie auf  **Speichern**.

Die ARIS Publisher-Integration wird aktiviert.

TEST DURCHFÜHREN

1. Melden Sie sich bei ARIS Risk & Compliance Manager mit der Rolle **Test-Manager** an.
2. Öffnen Sie ein Risiko, welches durch den Stammdatendateiimport generiert wurde.
3. Klicken Sie in der Zeile **Funktion** auf **Objektverknüpfung** und **Modellverknüpfung**.

ARIS Publisher wird in einem neuen Fenster geöffnet. Das entsprechende Objekt oder Modell wird geöffnet, wenn die Anbindung korrekt konfiguriert wurde.

2.5 Runnable über ARIS Cloud Controller sichern und rücksichern

ARIS Risk & Compliance Manager ermöglicht das Generieren und Rücksichern von Datenbankschnappschüssen direkt aus der Web-Anwendung. Die ARIS Cloud Controller (ACC)-Funktionalität zum Sichern und Rücksichern von Mandanten ist zusätzlich zum Generieren von Runnable-Sicherungsdateien verwendbar, die einen Datenbankschnappschuss sowie alle angewandten individuellen Anpassungen enthalten. Nähere Informationen finden Sie im Handbuch für das **ARIS Cloud Controller (ACC)-Kommandozeilenprogramm** in den Kapiteln **Back up a tenant** und **Restore a tenant**.

2.6 Runnable über ARIS Tenant Management sichern und rücksichern

ARIS Tenant Management erlaubt die Sicherung und Rücksicherung mandantenspezifischer Daten von ARIS Risk & Compliance Manager. Die erzeugten Runnable-Sicherungsdateien enthalten einen Datenbankschnappschuss sowie alle angewandten individuellen Anpassungen. Nähere Informationen finden Sie im **ARIS Tenant Management Handbuch**.

Hinweis: Bei der Rücksicherung mandantenspezifischer Daten über ARIS Tenant Management müssen die Sicherungsdateien dieselben individuellen Anpassungen enthalten wie die angewandten Exemplare von ARIS Risk & Compliance Manager. Ist dies nicht der Fall, sind die individuellen Anpassungen für die entsprechenden Exemplare manuell anzuwenden.

2.7 ARCM mit anderen Mandanten als dem 'Standard'-Mandanten verwenden

Wenn ARIS Risk & Compliance Manager für einen anderen Mandanten als den **Standard**-Mandanten konfiguriert ist, muss der Mandantename in der URL für den Zugriff auf ARIS Risk & Compliance Manager enthalten sein. Nach der Anmeldung wird der Mandantename nicht mehr in der URL angezeigt.

Beispiel





URL für Zugriff auf ARIS Risk & Compliance Manager mit Mandant **umg**:

<https://<servername>:<port>/arcm/login.jsp?tenant=umg>

2.8 Sprachen in ARIS Administration wählen


Wenn ARIS Risk & Compliance Manager in derselben Infrastruktur ausgeführt wird wie ARIS Connect, können die verfügbaren Sprachen in ARIS Administration konfiguriert werden. Standardmäßig stehen die folgenden Sprachen zur Verfügung: Deutsch, Englisch, Französisch, Chinesisch, Japanisch, Spanisch, Portugiesisch, Italienisch, Magyarisch, Arabisch. Sie können Sprachen deaktivieren, sodass sie nicht mehr in ARIS Risk & Compliance Manager und ARIS Connect verfügbar sind. Wenn nur Sprachen konfiguriert sind, die ARIS Risk & Compliance Manager nicht unterstützt, wird auf Englisch zurückgegriffen.

Vorgehen

1. Starten Sie ARIS Connect.
2. Melden Sie sich als **Systembenutzer** an.
3. Klicken Sie auf  **Anwendungsstarter** >  **Administration. ARIS Administration** wird geöffnet.
4. Klicken Sie auf **Konfigurations-Sets verwalten**. Alle verfügbaren Konfigurations- und Änderungs-Sets werden angezeigt. Das aktuelle Konfigurations- oder Änderungs-Set ist als **(aktiv)** gekennzeichnet. Bearbeiten Sie ein vorhandenes Änderungs-Set oder erstellen Sie ein neues. Sie können nur benutzerdefinierte Änderungs-Sets bearbeiten. Detaillierte Informationen, wie etwa zum Erstellen eines Änderungssets, finden Sie in der Online-Hilfe von ARIS Connect.
5. Halten Sie den Mauszeiger über das entsprechende Änderungs-Set und klicken Sie auf  **Bearbeiten**. Die Seite **Änderungs-Set definieren** wird geöffnet und Sie können das Änderungs-Set bearbeiten.
6. Klicken Sie auf **Sprachen wählen**.
7. Wählen Sie in der Liste **Aktuelle Sprache** die Sprachen aus, die Sie nicht benötigen, und klicken Sie dann auf **Deaktivieren**. Die ausgewählten Sprachen werden in die Liste **Weitere Sprachen** aufgenommen.
8. Wählen Sie in der Liste **Weitere Sprachen** die Sprachen aus, die Sie benötigen, und klicken Sie dann auf **Aktivieren**. Die Sprachen werden in die Liste **Aktuelle Sprache** aufgenommen.
9. Klicken Sie auf **Anwenden**.
10. Klicken Sie auf  **Zurück**.
11. Aktivieren Sie das Änderungs-Set, sofern es nicht bereits aktiviert ist, etwa im Fall, dass Sie ein neues Änderungs-Set erstellt haben.

Die in der Liste **Aktuelle Sprache** aufgeführten Sprachen können von den ARIS Risk & Compliance Manager- und ARIS Connect-Benutzern ausgewählt werden.

2.9 Anpassen der Zeitplanung

ARIS Risk & Compliance Manager bietet grundsätzlich zwei Möglichkeiten, automatisierte Server-Tasks zu starten, um Objekte zu generieren oder zu verändern. Wenn Sie über die entsprechende Managerrolle verfügen, können Sie in ARIS Risk & Compliance Manager ( **Administration > Server-Tasks**) einen Server-Task manuell anstoßen. Ansonsten werden die Server-Tasks von ARIS Risk & Compliance Manager zu den geplanten Zeiten automatisch ausgeführt. In der Standardkonfiguration ist das beispielsweise für die Generator- und Überwachungs-Server-Tasks der Fall.

Server-Task-Konfigurationsparameter beginnen stets mit **arcm.config.schedule.job**, gefolgt vom Server-Task-Typ (Generator, Monitor, Updater) und dann vom Objekttyp, für den der Server-Task verantwortlich ist, z. B. **arcm.config.schedule.job.generator.testcase**. Der Cleaning-Server-Task verfügt nicht über diesen Objekttyp-Anhang:

arcm.config.schedule.job.cleaning. Der Wert eines Server-Task-Parameters besteht aus einer Abfolge von Schlüsselwertpaaren, die durch eckige Klammern `[]` zu Gruppen zusammengefasst sind. Schlüssel und Wert sind durch einen senkrechten Strich `(|)` voneinander getrennt. Um die Einstellungen der geplanten Server-Tasks in ARIS Risk & Compliance Manager zu ändern, gehen Sie wie folgt vor. Weitere Informationen finden Sie in der CronTrigger-Dokumentation auf der Quartz-Homepage (<http://www.quartz-scheduler.org>).

Beispiele

- Der Generator-Server-Task für Kontrolltests soll jeden Tag um 00:52 gestartet werden. Der Server-Task soll für alle Umgebungen ausgeführt werden, außer der Umgebung **env1**.

Eigenschaftsschlüssel:

```
arcm.config.schedule.job.generator.testcase
```

Wert:

```
[ jobitem | generatorJob ] [ startScheduler | true ] [ executionTime | 0 52 00 ? * SUN-SAT ] [ excludedEnvironments | env1 ] [ includedEnvironments | ] [ objecttypes | TESTCASE ]
```

- Der Überwachungs-Server-Task für Risikobewertungen soll von Montag bis Freitag um 08:00 und um 18:00 gestartet werden. Der Server-Task soll nur für die Umgebung **env1** ausgeführt werden.

Eigenschaftsschlüssel:

```
arcm.config.schedule.job.monitor.riskassessment
```

Wert:

```
[ jobitem | monitorJob ] [ startScheduler | true ] [ executionTime | 0 8,18 ? * MON-FRI ] [ excludedEnvironments | ] [ includedEnvironments | env2 ] [ objecttypes | RISKASSESSMENT ]
```

BEDEUTUNG DER EINZELNEN PARAMETER

JOBITEM

Der Server-Task, der ausgeführt werden soll. Der Parameterwert muss einer EnumItem-ID aus der Aufzählung **jobs** in der Datei **enumerations.xml** entsprechen.

STARTSCHEDULER

Der Wert muss **true** sein, damit die Zeitsteuerung für diesen Server-Task aktiv ist.

EXECUTIONTIME

Dieser Ausdruck legt fest, wann der Server-Task gestartet werden soll. Er hat das Format **CronTrigger**, welches die Angabe von Zeitintervallen erlaubt. Von links nach rechts bedeuten die einzelnen Werte:

- **Seconds** (0-59)
- **Minutes** (0-59)
- **Hours** (0-23)
- **Day of month** (1-31 oder Fragezeichen (?) für einen beliebigen Kalendertag des Monats)
- **Month** (1-12, JAN-DEZ, oder Sternchen (*) für einen beliebigen Monat)
- **Day of week** (1-7 oder SUN-SAT)
- **Year** (kann leer sein, 1984, 1970-2099, ...)

EXCLUDEENVIRONMENTS

Hier werden die Umgebungen innerhalb der Datenbank von ARIS Risk & Compliance Manager angegeben, für die der Server-Task nicht ausgeführt werden soll. Die Werte können durch Kommas getrennt angegeben werden. Dies gilt nur für umgebungsspezifische Server-Aufträge.

INCLUDEENVIRONMENTS

Hier werden die Umgebungen innerhalb der Datenbank von ARIS Risk & Compliance Manager angegeben, für die der Server-Task ausgeführt werden soll. Ist kein Wert festgelegt, wird für jede einzelne Umgebung ein separater Server-Task gestartet. Die Werte können durch Kommas getrennt angegeben werden. Dies gilt nur für umgebungsspezifische Server-Aufträge.

OBJECTTYPES



Die Objekttypen, für die der Server-Task ausgeführt werden soll. Im obigen Beispiel soll diese Instanz des Überwachungs-Server-Task ausschließlich die Kontrolltests überprüfen. Die Werte können durch Kommas getrennt angegeben werden.

GEPLANTE SERVER-TASKS KONFIGURIEREN

Voraussetzung

Sie haben die Rolle **Systemadministrator**.

Vorgehen

1. Klicken Sie auf  **Administration**. Das Menüelement **Allgemein** wird anfänglich angezeigt.
2. Klicken Sie unter **Systemmanagement** auf **Systemkonfiguration**. Die Konfigurationsparameter werden angezeigt.
3. Um die zeitgesteuerten Server-Tasks anzuzeigen, filtern Sie die Systemkonfiguration nach **Administration > Server-Task-Zeitpläne**. Das Suchergebnis zeigt alle zeitgesteuerten Server-Tasks mit ihren aktuellen Werten an.
4. Klicken Sie in der Zeile des Parameters, den Sie ändern möchten, auf  **Bearbeiten**. Der Dialog **Parameterwert setzen** wird geöffnet.

5. Kopieren Sie **Current value** in die Zwischenablage. Zum Beispiel:

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


6. Fügen Sie den Wert in einen Texteditor ein und nehmen Sie eine relevante Änderung vor, ändern Sie z. B. die Ausführungszeit. Zum Beispiel:

```
[ jobitem | generatorJob ] [ startScheduler | true ] [ executionTime |
0 0 8-18 ? * MON-FRI ] [ excludedEnvironments | ] [ includedEnvironments
| ] [ objecttypes | TESTCASE ]
```

7. Kopieren Sie den geänderten Parameter in die Zwischenablage und fügen Sie ihn in das Textfeld **New value** ein.

Stellen Sie sicher, dass Sie immer den vollständigen String kopieren und einfügen. Sie können nicht nur einen Teil des Strings verwenden, den Sie anpassen wollen, z. B. `executionTime | 0 0 8-18 ? * MON-FRI]`.

8. Klicken Sie auf **OK**.

Die Änderungen werden sofort übernommen und in der Datenbank gespeichert. Klicken Sie in der Zeile des entsprechenden Parameters auf  **Zurücksetzen**, um ihn auf den Standardwert zurückzusetzen.

3 Glossar

Im Glossar sind grundlegende Fachbegriffe erklärt.

GLOBAL UNIQUE IDENTIFIER (GUID)

Eindeutiger, datenbankübergreifender Identifizierer für Elemente von ARIS.

JAVA DATABASE CONNECTIVITY (JDBC)

Schnittstelle, die die Kommunikation zwischen einer Java-Anwendung und einer Datenbank ermöglicht.

MULTI-PURPOSE INTERNET MAIL EXTENSIONS-MAPPING (MIME-MAPPING)

Verbindet eine Dateinamenerweiterung mit dem Typ der Datendatei, z. B. Text, Audio, Bild.

SERVICE-ID VON ORACLE (SID)

Eindeutige Kennung, die Oracle benötigt, um die Datenbankinstanz zu identifizieren.

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

Übertragungsprotokoll speziell für den Austausch von Mails. Es legt beispielsweise fest, wie zwei Mailssysteme interagieren und wie die Steuermeldungen zu diesem Zweck aussehen müssen.

SINGLE SIGN-ON (SSO)

Durch die Einmalanmeldung (Single Sign-On, SSO) braucht sich ein Benutzer nur einmal mit Benutzername und Kennwort zu authentifizieren, um ohne erneute Anmeldung auf alle Dienste, Programme und Rechner zuzugreifen. Wenn Dienste, Programme und Rechner eine erneute Authentifizierung verlangen, wird diese durch den zugrunde liegenden SSO-Mechanismus vorgenommen.

4 Rechtliche Hinweise

4.1 Dokumentationsumfang

Die zur Verfügung gestellten Informationen beschreiben die Einstellungen und Funktionalitäten, die zum Zeitpunkt der Veröffentlichung gültig waren. Da Software und Dokumentation verschiedenen Fertigungszyklen unterliegen, kann die Beschreibung von Einstellungen und Funktionalitäten von den tatsächlichen Gegebenheiten abweichen. Informationen über solche Abweichungen finden Sie in den mitgelieferten Release Notes. Bitte lesen und berücksichtigen Sie diese Datei bei Installation, Einrichtung und Verwendung des Produkts.

Wenn Sie technische und/oder geschäftliche Systemfunktionen ohne Nutzung der Service-Leistungen der Software AG installieren möchten, benötigen Sie umfangreiche Kenntnisse hinsichtlich des zu installierenden Systems, seines Zwecks sowie der Zielsysteme und ihrer Abhängigkeiten untereinander. Aufgrund der Anzahl an Plattformen und voneinander abhängigen Hardware- und Software-Konfigurationen können wir nur spezifische Installationen beschreiben. Es ist nicht möglich, sämtliche Einstellungen und Abhängigkeiten zu dokumentieren.

Beachten Sie bitte gerade bei der Kombination verschiedener Technologien die Hinweise der jeweiligen Hersteller, insbesondere auch aktuelle Verlautbarungen auf deren Internet-Seiten bezüglich Freigaben. Für die Installation und einwandfreie Funktion freigegebener Fremdsysteme können wir keine Gewähr übernehmen und leisten daher keinen Support. Richten Sie sich grundsätzlich nach den Angaben der Installationsanleitungen und Handbücher der jeweiligen Hersteller. Bei Problemen wenden Sie sich bitte an die jeweilige Herstellerfirma.

Falls Sie bei der Installation von Fremdsystemen Hilfe benötigen, wenden Sie sich an Ihre lokale Software AG-Vertriebsorganisation. Beachten Sie bitte, dass solche Hersteller- oder kundenspezifischen Anpassungen nicht dem Standard-Softwarepflege- und Wartungsvertrag der Software AG unterliegen und nur nach gesonderter Anfrage und Abstimmung erfolgen.

Bezieht sich eine Beschreibung auf ein spezifisches ARIS-Produkt, wird dieses genannt. Andernfalls werden die Bezeichnungen für die ARIS-Produkte folgendermaßen verwendet:

Name	Umfasst
ARIS-Produkte	Bezeichnet sämtliche Produkte, für die die Lizenzbedingungen der Software AG-Standard-Software gelten.
ARIS-Clients	Bezeichnet alle Programme, die über ARIS Server auf gemeinsam verwendete Datenbanken zugreifen, z. B. ARIS Architect oder ARIS Designer.

Name	Umfasst
ARIS-Download-Clients	Bezeichnet ARIS-Clients, die aus dem Browser gestartet werden können.

5 Index

B

Benutzer

Aktualisierung in ARIS Risk &
Compliance Manager • 9

Export aus ARIS Architect • 6

Import ins User Management • 7

E

Einleitung • 2

Event-Enabling • 3

G

GLOBAL UNIQUE IDENTIFIER (GUID) • 19

J

JAVA DATABASE CONNECTIVITY (JDBC) •
19

L

LDAP • 10

M

Mandant • 14

MULTI-PURPOSE INTERNET MAIL
EXTENSIONS-MAPPING • 19

S

SERVICE-ID VON ORACLE • 19

Sichern und Wiederherstellen

Über ARIS Cloud Controller • 14

Über ARIS Tenant Management • 14

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)
• 19

V

Verzeichnisdienst anbinden • 10