

ARIS

# CLOUD CONTROLLER (ACC) COMMAND-LINE TOOL

VERSION 10.0 - SERVICE RELEASE 18  
MAY 2022

This document applies to ARIS 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 - 2022 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).

# Contents

Contents.....	1
1 ARIS Cloud Controller (ACC).....	1
1.1 How to start ARIS Cloud Controller (ACC).....	2
1.2 How to connect nodes.....	4
1.3 How to list runnables .....	5
1.4 How to handle special characters.....	6
1.5 What runnables are available? .....	7
1.6 Security advice.....	12
1.6.1 Safety recommendation: Block AJP ports.....	12
1.6.2 Check open AJP ports (Ghostcat vulnerability) .....	13
1.7 Use cases.....	15
1.7.1 Change the default agent user's password.....	15
1.7.2 Start and stop runnables .....	16
1.7.3 Deactivate runnable.....	16
1.7.4 Activate runnable .....	16
1.7.5 Provide additional memory .....	17
1.7.6 Reconfigure autostart settings .....	18
1.7.7 Make TLS certificate available for ARIS Server .....	19
1.7.8 Redirect ports.....	20
1.7.9 Redirect HTTPS port .....	21
1.7.10 Collect log files (ACC) .....	22
1.7.11 Delete log files.....	22
1.7.12 ARIS Administration/ARIS Risk and Compliance.....	24
1.7.12.1 Specify a white list for ARIS Administration.....	24
1.7.12.2 Use existing ARIS document storage and ARIS Administration for ARIS Risk and Compliance .....	25
1.7.13 Process Governance.....	26
1.7.14 ARIS Aware.....	27
1.7.14.1 Make enhancements available .....	27
1.7.15 ARIS Publisher .....	28
1.7.15.1 Provide ARIS Publisher license files .....	28
1.7.15.2 Reconfigure settings .....	29
1.7.15.3 Configure the service 'Create static ARIS Publisher export' for Process Governance .....	31
1.7.16 Collaboration .....	32
1.7.16.1 Specify a black list for Collaboration .....	32
1.7.16.2 Create synchronization user .....	33
1.7.16.3 Anonymize Collaboration user.....	33
1.7.16.4 Force synchronize Collaboration users .....	34
1.7.17 Tenant Management.....	35
1.7.17.1 Create a tenant .....	35
1.7.17.2 Back up a tenant.....	36
1.7.17.3 Delete a tenant.....	38
1.7.17.4 Restore a tenant .....	39
1.7.17.5 What data is backed up and restored?.....	40

1.7.17.6	Copy a tenant to a different server .....	43
1.7.17.7	How to adjust timestamps related to ARIS document storage.....	45
1.7.18	Database connection.....	46
1.7.18.1	Provide JDBC drivers.....	46
1.7.18.2	Update external service (database clusters) .....	47
1.7.18.3	Configure the database connection for additional schemes .....	48
1.7.18.4	Move the database management system.....	50
1.7.19	Elasticsearch .....	52
1.7.19.1	Check user name and password (Elasticsearch).....	52
1.7.19.2	Change user name and password (Elasticsearch).....	53
1.7.19.3	Disable authentication for Elasticsearch .....	53
1.7.20	Health check.....	54
1.7.20.1	Show node.....	54
1.7.20.2	Monitor runnable's health .....	55
1.7.20.3	Configure health monitoring.....	56
1.7.21	Mailing.....	59
1.7.21.1	Configure ARIS Agent mail server connection.....	59
1.7.21.2	Configure SMTP mail server connection .....	61
1.7.22	Third-party document management systems (TDMS) .....	63
1.7.22.1	Make TDMS available.....	63
2	Legal information.....	64
2.1	Documentation scope.....	64
2.2	Support .....	64

## 1 ARIS Cloud Controller (ACC)

ACC is a command-line tool (see ARIS Cloud Controller (ACC) Command-Line Tool.pdf (../../documents/3 Installation/31 Initial installation/312 Server/3121 Basic (Single node)/ARIS Cloud Controller (ACC) Command-Line Tool.pdf)) for administrating and configuring an ARIS installation. It communicates with ARIS Agents on all nodes. You can use it in multiple modes.

## 1.1 How to start ARIS Cloud Controller (ACC)

ACC is a command-line tool (see ARIS Cloud Controller (ACC) Command-Line Tool.pdf ([../documents/3 Installation/31 Initial installation/312 Server/3121 Basic \(Single node\)/ARIS Cloud Controller \(ACC\) Command-Line Tool.pdf](#))) for administrating and configuring an ARIS installation. It communicates with ARIS Agents on all nodes.

### Warning

Using ACC commands will deeply affect your system. This requires profound knowledge of the technical ARIS infrastructure and environment. The required know-how can be acquired only by attending the training course **ARIS Server Installation**, available via Global Education Services (<https://softwareag.com/training>). If you use ACC commands without this knowledge or without the services of Software AG, according to the standard Software AG software maintenance agreement, we cannot guarantee proper functioning.

ARIS Cloud Controller (ACC) can be used in three modes:

### INTERACTIVE MODE (DEFAULT)

ACC runs with an interactive shell, allowing you to manually issue commands.

### BATCH MODE

Activated by specifying a command file with the **-f** command line parameter (see ACC command line parameters below). ACC will execute the commands in the file in the given sequence and exit after execution or if one of the commands fails.

A command file line starting with **#** will be interpreted as a comment line and ignored by ACC.

### COMMAND MODE

You can directly pass a single command to ACC as a command line parameter. The command will be executed and ACC will exit afterwards.

When passing commands directly as a command line parameter, you must be careful when escaping strings in your command, for example, double-quote-delimited parameters. The operating system command shell will consume the double quotes, leaving your string parameter un-escaped. So please escape the quote characters and special characters.



## Examples

If you issue the command in command mode, for example:

```
set remote.repository.url="http://something.com/repo"
```

You must enter:

```
acc.bat -h localhost -u <user name> -pwd <remoteAccessPassword> set  
remote.repository.url=\"http://something.com/repo\"
```

If you enter:

```
acc.bat -h localhost -u <user name> -pwd <remoteAccessPassword> set  
remote.repository.url="http://something.com/repo"
```

ACC will return an error message, for example:

```
line 1:52 mismatched character '<EOF>' expecting '\n'  
Invalid or erroneous command "set  
remote.repository.url=http://something.com/repo ": line 1:30 extraneous  
input ':' expecting EOF  
Use "help" to display a list of available commands.
```

This also affects passwords and names containing special characters. If you try to back up your tenants using the following command, make sure to escape the quote characters and the special character **&** used in the password **User&12345**.

If your username or password includes any special character, add a backslash (\) before the character for ACC to process the special character as a string. That is, if there is an ampersand (&), in your password, add a backslash before the ampersand.

```
./acc.bat -h localhost -u Clous -pwd g3h31m -p 18011 -c  
../generated.apptypes.cfg backup tenant default username=\"admin\  
password=\"User\&12345\"
```

To get information about the usage of ACC commands, enter **help** or **help <command>**.

## WINDOWS OPERATING SYSTEM

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.

## LINUX OPERATING SYSTEM

To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead. To do so, enter: **su -c acc10.sh aris10**. After the ARIS Server installation has completed on a Linux operating system, the **aris10** user is locked and has no password. Command-line tools (**sh** files), such as **ARIS Server Administrator** or **ARIS Cloud Controller** can only be started by the **aris10** user related to the ARIS Agent.

- To unlock the **aris10** user, enter: **passwd -u aris10**
- To interactively enter a password, enter: **passwd aris10**
- To start the command-line tools, enter: **su -c acc10.sh aris10** or **su -c arisadm.sh aris10**
- To execute these command-line tools as an ARIS user that has no **root** privileges, you must enter the password of the **aris10** user.
- To copy files manually into the **ARIS** directory, as the **aris10** user use the commands: **su aris10** and **sudo aris10**

As an ARIS user that has no **root** privileges, you must make sure that the files have the correct ownership (**aris10**).

- To lock the **aris10** user again enter: **passwd -l aris10**

## 1.2 How to connect nodes

When you start ACC in one of the three usage modes without any additional command line parameter, it will by default connect to the node installed by the setup program. There are three options to specify nodes you want to control with ACC:

- You can use the **add node** command to put the individual cloud nodes under ACC's control. This requires profound knowledge of the technical ARIS infrastructure and environment. The required know-how can be acquired only by attending the training course **ARIS Server Installation**.
- Alternatively, you can list all your cloud nodes in a node file and pass this file to the ACC with the **\-n** (or **--nodefile**) command line option.
- If you only want to connect to a single node and issue commands there, you can also use the ACC's **-h** (or **--host**) command line option to directly specify the host or IP name of the node you want to control with ACC.



## 1.3 How to list runnables

Start ACC and enter **list** to monitor the status of all runnables. This example shows ACC of a current ARIS Server installation for a medium number of users.

```
ACC+ localhost>list
Node localhost - 16 installed runnables.
ID                               State  Version  Type
zoo_m                             STARTED 10.0.18.0 com.aris.runnables.zookeeper-run-prod
postgres_m                         STARTED 10.0.18.0 com.aris.runnables.PostgreSQL-run-prod
cloudsearch_m                      STARTED 10.0.18.0 com.aris.cip.y-cloudsearch-run-prod
elastic_m                          STARTED 10.0.18.0 com.aris.runnables.elasticsearch-run-prod
umcadmin_m                         STARTED 10.0.18.0 com.aris.umcadmin.y-umcadmin-run-prod
adsadmin_m                         STARTED 10.0.18.0 com.aris.adsadmin.y-adsadmin-run-prod
abs_m                              STARTED 10.0.18.0 com.aris.modeling.components.y-server-run-prod
octopus_m                          STARTED 10.0.18.0 com.aris.octopus.y-octopus_server-run-prod
apg_m                              STARTED 10.0.18.0 com.aris.age.age-run-prod
copernicus_m                       STARTED 10.0.18.0
com.aris.copernicus.copernicus-portal-server-run-prod
ecp_m                              STARTED 10.0.18.0 com.aris.runnables.ecp-run-prod
simulation_m                       STARTED 10.0.18.0
com.aris.modeling.components.simulationserver.y-simuserver-run-prod
loadbalancer_m                    STARTED 10.0.18.0 com.aris.runnables.httpd.httpd-run-prod
dashboarding_m                   STARTED 10.0.18.0 com.aris.dashboarding.dashboarding-run-prod
businesspublisher_m             STARTED 10.0.18.0
com.aris.modeling.components.businesspublisher.y-bp-server-run-prod
arcm_m                            STARTED 10.0.18.0 com.aris.arcm.arcm-run-prod
```

The state of all runnables represented by their instance IDs is listed. Possible states are:

- **UNKNOWN:** The runnable state is not yet known. This state is shown directly after ARIS Agent was started.
- **STOPPED:** The runnable is currently not running.
- **STARTING:** The runnable is starting, but this process is not complete yet.
- **STARTED:** The runnable is running.
- **STOPPING:** The runnable is stopping, but this process is not complete yet.
- **DEACTIVATED:** The runnable is not in use. It has been deactivated manually and can be activated if necessary. If the **dashboarding** runnable is in this state, that does not have to be an error. This runnable is deactivated if ARIS Server was installed without ARIS Aware.
- **DOWN:** This runnable started and crashed. ARIS Agent will attempt to automatically restart the runnable momentarily.
- **FAILED:** This runnable has crashed. ARIS Agent has given up trying to restart the runnable.

If a runnable does not start properly, read the **Basic Troubleshooting** guide.

## 1.4 How to handle special characters

If you pass a command to a command-line tool, such as ARIS Cloud Controller, special characters used in names, passwords, or user names may cause issues.

When passing commands directly as a command line parameter, you must be careful when escaping strings in your command, for example, double-quote-delimited parameters. The operating system command shell will consume the double quotes, leaving your string parameter un-escaped. So please escape the quote characters and special characters.

### Examples

If you issue the command in command mode, for example:

```
set remote.repository.url="http://something.com/repo"
```

You must enter:

```
acc.bat -h localhost -u <user name> -pwd <remoteAccessPassword> set  
remote.repository.url="\http://something.com/repo\"
```

If you enter:

```
acc.bat -h localhost -u <user name> -pwd <remoteAccessPassword> set  
remote.repository.url="http://something.com/repo"
```

ACC will return an error message, for example:

```
line 1:52 mismatched character '<EOF>' expecting '\n'  
Invalid or erroneous command "set  
remote.repository.url=http://something.com/repo ": line 1:30 extraneous  
input ':' expecting EOF  
Use "help" to display a list of available commands.
```

This also affects passwords and names containing special characters. If you try to back up your tenants using the following command, make sure to escape the quote characters and the special character **&** used in the password **User&12345**.

If your username or password includes any special character, add a backslash (\) before the character for ACC to process the special character as a string. That is, if there is an ampersand (&), in your password, add a backslash before the ampersand.

```
./acc.bat -h localhost -u Clous -pwd g3h31m -p 18011 -c  
../generated.apptypes.cfg backup tenant default username=\"admin\  
password=\"User\&12345\"
```

## 1.5 What runnables are available?

This table lists all runnables run by ARIS Server for a medium number of users installation. That's why all runnables end with **\_m**. Installations for a small or a large number of users are typified with **\_s** or **\_l**. If ARIS was installed using the setup program, the default instance IDs are used as shown in the table.

Runnable	ARIS Server	ARCM
	Runnables run by different server types	
Instance ID: <b>zoo_m</b> Name: Service registry Description: This runnable is a server component managing the communication, configuration and status information of all available runnables and external services.	x	x
Instance ID: <b>postgres_m</b> Name: Modeling database Description: Internal standard database system storing all ARIS databases (modeling data) and the system databases (ARIS method, filters, templates, languages, fonts, font formats and script data). This database can be replaced by an external Oracle® or Microsoft® SQL database.	x	x
Instance ID: <b>cloudsearch_m</b> Name: Search index Description: Main full-text search and graph structure index for modeling data. It allows fast access to the data stored in the modeling database, Oracle® or Microsoft® SQL database.	x	x

Runnable	ARIS Server	ARCM
<p>Instance ID: <b>elastic_m</b></p> <p>Name: Document index (Elasticsearch)</p> <p>Description: Main full-text search index for documents and collaboration data. It also stores users, user groups, licenses, and privileges.</p>	x	x
<p>Instance ID: <b>adsadmin_m</b></p> <p>Name: ARIS document storage management</p> <p>Description: Server component managing ARIS document storage.</p>	x	x
<p>Instance ID: <b>umcadmin_m</b></p> <p>Name: ARIS Administration/User Management</p> <p>Description: Server component managing users, permissions, licenses, LDAP connectivity and SSO.</p>	x	x
<p>Instance ID: <b>loadbalancer_m</b></p> <p>Name: Load balancer</p> <p>Description: Central point of entry for all ARIS clients to the entire ARIS application, typically accessed via HTTP ports 80 or 1080, or HTTPS ports 443 or 1443. It distributes the workload across the installed components.</p>	x	x
<p>Instance ID: <b>abs_m</b></p> <p>Name: Main server component</p> <p>Description: Server component for modeling, publishing, and operations on modeling data including report execution.</p>	x	x
<p>Instance ID: <b>apg_m</b></p> <p>Name: Process Governance</p> <p>Description: Process Governance server component. Executes processes and provides managing user interfaces.</p>	x	

Runnable	ARIS Server	ARCM
<p>Instance ID: <b>copernicus_m</b></p> <p>Name: Portal</p> <p>Description: Server component providing the portal in ARIS.</p>	x	
<p>Instance ID: <b>octopus_m</b></p> <p>Name: Analysis</p> <p>Description: Server component processing ad hoc analyses and queries triggered in ARIS Architect or ARIS Designer.</p>	x	
<p>Instance ID: <b>ecp_m</b></p> <p>Name: Collaboration</p> <p>Description: Server component of the collaboration component in ARIS.</p>	x	
<p>Instance ID: <b>simulation_m</b></p> <p>Name: Simulation</p> <p>Description: Server component of the simulation functionality in ARIS Architect.</p>	x	
<p>Instance ID: <b>dashboarding_m</b></p> <p>Name: Dashboards (ARIS Aware)</p> <p>Description: Server component of the dashboarding component in ARIS.</p>	x	

Runnable	ARIS Server	ARCM
<p>Instance ID: <b>businesspublisher_m</b></p> <p>Name: ARIS Publisher server</p> <p>Description: Server component of the ARIS Publisher functionality in ARIS Architect.</p>	<p>From ARIS 10.0.13.0 on ARIS Publisher and IT Inventory are no longer delivered. This means that you can no longer install or update ARIS Publisher Server. You can still use your current ARIS Publisher installation, but since this component is no longer supported, no more features will be developed. We strongly recommend using the ARIS portal (Published content) instead of ARIS Publisher in the future.</p>	
<p>Instance ID: <b>arcm_m</b></p> <p>Name: ARIS Risk and Compliance server</p> <p>Description: Server component of ARIS Risk and Compliance.</p>		x
<p>Instance ID: <b>hds_m</b> (optional; not by setup)</p> <p>Name: Heavy-duty Server (HDS)</p> <p>Description: HDS is an additional component that reduces the load of ARIS reports running on you <b>abs</b> instance.</p>	x	
<p>Instance ID: <b>cdf_m</b> (optional; not by setup)</p> <p>Name: Cloud Decoupling Framework (CDF)</p> <p>Description: CDF is a queue that can be used to decouple synchronous accesses to services. It is required for communication between the <b>abs</b> instance and the <b>hds</b> instance.</p> <p>If multiple <b>arcm</b> runnables are installed, a <b>cdf</b> runnable is mandatory.</p>	x	



Runnable	ARIS Server	ARCM
<p>Instance ID: <b>ces_m</b> (optional; not by setup) Name: Enterprise search (CES) Description: CES is an extension that provides the powerful enterprise search.</p>	<p>x</p>	

## 1.6 Security advice

Due to the Tomcat (Ghostcat) vulnerability, you are recommended to block (page 12) access to all **AJP** ports if you use an ARIS version prior to **10.0.12.0**.

### 1.6.1 Safety recommendation: Block AJP ports

The **Apache JServ Protocol** (AJP) is a binary protocol that can proxy incoming requests from a web server to an application server behind the web server. AJP is a highly trusted protocol. It must not be made available to untrusted clients because they could gain access to confidential information or execute code on the application server.

ARIS uses AJP for communication between the **loadbalancer** runnable that bases on Apache HTTPD and ARIS applications that base on Apache Tomcat. The vulnerable Tomcat AJP connector is mandatory and must stay active for ARIS applications.

If you have installed ARIS Server according to our recommendations, you can block access to the ports of all runnables except the HTTP and HTTPS ports used by the **loadbalancer** runnable by setting appropriate firewall rules. By default these HTTP and HTTPS ports are **80** and **443** on Windows operating systems and **1080** and **1443** on Linux operating systems.

To prevent unauthorized access, check that the **AJP** ports of your ARIS installations are only accessible from networks from which users access ARIS (page 13). The **show node ACC** command gives an overview of open **AJP** ports. It lists all ports used by ARIS runnables. The **connector.ajp.port** parameter (in former ARIS versions called **CATALINA\_AJP\_PORT**) identifies **AJP** ports. If any of these ports are accessible from an external network, you must block access immediately by your firewall.

Important: If your ARIS system is a multiple node installation, the **AJP** ports must remain open for data transfer between multiple nodes. These open **AJP** ports do not represent a security gap, because distributed ARIS installations must always be protected by a firewall.

## 1.6.2 Check open AJP ports (Ghostcat vulnerability)

To prevent unauthorized access, check that the **AJP** ports of your ARIS installations are only accessible from networks from which users access ARIS (page 13).

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To check ports used by runnables, enter: **show node**

The list is displayed. Navigate to the **Known used ports section**.

Port	Runnable	Port Parameter	
443	loadbalancer_m	HTTPD.ssl.port	Set explicitly
1080	loadbalancer_m	HTTPD.port	Set explicitly
14200	cloudsearch_m	zookeeper.application.instance.port	Set explicitly
14201	cloudsearch_m	JAVA-DCSHTTTPORT	Set explicitly
14206	cloudsearch_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14220	elastic_m	ELASTICSEARCH.http.port	Set explicitly
14226	elastic_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14230*	elastic_m	ELASTICSEARCH.transport.tcp.port	Set explicitly
14240	postgres_m	postgresql.port	Set explicitly
14250	cdf_m	connector.http.port	Set explicitly
14251	cdf_m	<b>connector.ajp.port</b>	Set explicitly
14256	cdf_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14281	zoo_m	clientPort	DEFAULT
14296	zoo_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14400	abs_m	connector.http.port	Set explicitly
14401	abs_m	<b>connector.ajp.port</b>	Set explicitly
14406	abs_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14410	adsadmin_m	connector.http.port	Set explicitly
14411	adsadmin_m	<b>connector.ajp.port</b>	Set explicitly
14416	adsadmin_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14420	apg_m	connector.http.port	Set explicitly
14421	apg_m	<b>connector.ajp.port</b>	Set explicitly
14426	apg_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14430	copernicus_m	connector.http.port	Set explicitly
14431	copernicus_m	<b>connector.ajp.port</b>	Set explicitly
14436	copernicus_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14440	ecp_m	connector.http.port	Set explicitly
14441	ecp_m	<b>connector.ajp.port</b>	Set explicitly
14446	ecp_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14450	hds_m	connector.http.port	Set explicitly
14451	hds_m	<b>connector.ajp.port</b>	Set explicitly
14456	hds_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14460	octopus_m	connector.http.port	Set explicitly
14461	octopus_m	<b>connector.ajp.port</b>	Set explicitly
14466	octopus_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14470	simulation_m	connector.http.port	Set explicitly
14471	simulation_m	<b>connector.ajp.port</b>	Set explicitly
14476	simulation_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14480	umcadmin_m	connector.http.port	Set explicitly
14481	umcadmin_m	<b>connector.ajp.port</b>	Set explicitly
14486	umcadmin_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14490	dashboarding_m	connector.http.port	Set explicitly
14491	dashboarding_m	<b>connector.ajp.port</b>	Set explicitly
14496	dashboarding_m	JAVA-Dcom.sun.management.jmxremote.port	Set explicitly
14497	dashboarding_m	JAVA-Xrunjdp\:\transport	Set explicitly

The highlighted **connector.ajp.port** Port parameter indicates all open AJP ports.

3. If any of these ports are accessible from an external network, you must block access immediately by your firewall.

You have secured the system.

Important: If your ARIS system is a multiple node installation, the **AJP** ports must remain open for data transfer between multiple nodes. These open **AJP** ports do not represent a security gap, because distributed ARIS installations must always be protected by a firewall.

## 1.7 Use cases

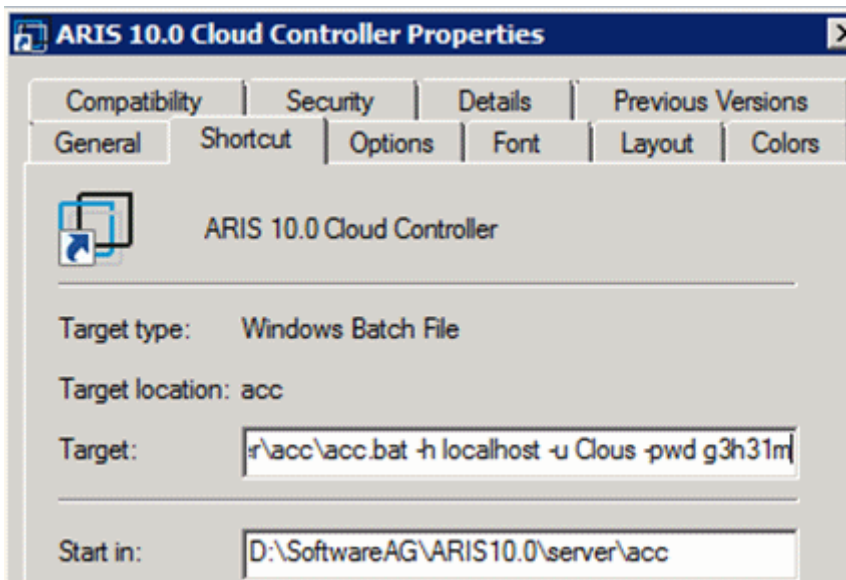
In these chapters product-related examples for configuring the system are available.

### 1.7.1 Change the default agent user's password

The ARIS Agent user has access to ARIS Cloud Controller (ACC). If you did not change the default password during the setup process you should do so manually to prevent unauthorized access.

#### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Change the password: **set password = "<enter the new password>"**
3. Stop ACC. Enter: **exit**
4. Restart ACC.
5. Enter the new password.
6. If you use the **Start** icon for ARIS Cloud Controller (**Start > All Programs > ARIS > Administration > ARIS Cloud Controller**) you can change the **password** command line parameter within the **ACC** shortcut. If you do not change the password it will be prompted every time you start ACC.



If you run an ARIS server setup after you have changed the password, enter the changed credentials.

## 1.7.2 Start and stop runnables

The start modus had been selected during the setup process. If you have chosen the option **Start automatically** all runnables will be started in the right order.

Runnables can also be started and stopped independently, but most runnables will not work on their own. You must start all needed runnables in the right order.

- Enter **startall** to get all runnables started in correct order.
- Enter **start <instanceld>**, for example, **start abs\_m** to start only the runnable **abs** (Modeling & Publishing (Business server)).
- Enter **stopall** to stop all runnables.
- Enter **stop <instanceld>**, for example, **stop abs\_m** to only stop one runnable.

If you run ARIS on a laptop (8 GB) for demonstration purposes you might want to stop runnables you do not need to ensure more memory for the system.

## 1.7.3 Deactivate runnable

Deactivation is useful, if you do not yet use a certain runnable, but maybe need it later. If you activate the runnables again, you can still use the setup program to update your ARIS version. To deactivate runnables is safer than removing or shutting them down.

A deactivated runnable cannot be started with a **start** command. They will be ignored by the **startall** command and the agent's runnable autostart.

### Prerequisites

Runnables are in **STOPPED** or **FAILED** state.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To deactivate the runnable enter, for example: **deactivate simulation\_m**

The **simulation** runnable will not be started, until you have activated it again (page 16).

## 1.7.4 Activate runnable

You can activate runnables that have been deactivated (page 16). This is required before starting an update setup.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).



2. To activate the runnable enter, for example: **activate simulation\_m**

The **simulation** runnable can be started again.

## 1.7.5 Provide additional memory

If you have performed an installation for small (s), medium (m) or large (l) memory requirement, you can provide additional memory for runnables.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Enter **reconfigure <runnable> +JAVA-Xmx=<memory requirement>**.

The affected runnables will be started after the settings have been updated.

### Examples

- **reconfigure abs\_s +JAVA-Xmx="1152m"**

The memory settings for the modeling runnable of an s installation will be increased to max. 1152 MB.

- **reconfigure abs\_m +JAVA-Xmx="6G"**

The memory settings for the modeling runnable of an m installation will be increased to 6 GB.

## 1.7.6 Reconfigure autostart settings

Using the **autostart.mode** parameter, you can reconfigure runnables to start automatically when the windows service starts. This parameter is used as a node setting valid for all runnables at a node. Do not use the **autostart.mode** parameter for runnables. For runnables use the **set runnable property** command to set their **autostart** parameter to **true**. If you do not want a runnable to be started, you must deactivate (page 16) it.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To change settings for one node, enter for example:

```
set autostart.mode="all"
```

To change settings for all nodes, enter for example:

```
on all nodes set autostart.mode="all"
```

You can use the following values:

**all:** starts all runnable automatically.

**off:** no runnable is started automatically.

**autostart.flag:** only those runnables which have their **autostart** set to **true** (by invoking the **set runnable property** command) are started automatically.

**last.started:** only those runnables that were started the last time are started automatically. These are all runnables for which an explicit **start** command had been issued, without being followed by an explicit **stop** or **kill** command.

Runnables are started automatically when ARIS Agent starts up, but only if the **autostart.mode** is set to **all**, **autostart.flag**, or **last.started** or if ARIS Agent finds all runnables to be either in state **STOPPED** or **UNKNOWN** after starting up. This prevents ARIS Agent from starting up runnables if ARIS Agent itself but not the entire node is manually restarted and the runnables themselves are still active.

## 1.7.7 Make TLS certificate available for ARIS Server

By default, the **loadbalancer** runnable is set to allow both unencrypted HTTP (port 80) and encrypted HTTPS (port 443) access. In order to use TLS (former SSL), the certificate must fit to the load balancer's host name. Otherwise, client connections in particular web browser connections will fail due to an invalid certificate.

### OBTAINING A VALID CERTIFICATE

If you want to use TLS, you need a valid certificate for the server on which the load balancer is running. This certificate must be signed by a certificate authority (CA). Please make sure that the certificate is compatible with the Java version of all ARIS clients.

- You can buy a certificate from an official CA. Most clients in particular browsers will trust certificates signed by such a CA.
- If your company uses own CA, use a certificate from this CA and add this CA to the trust store of all clients.

### ADDING A VALID CERTIFICATE TO THE LOAD BALANCER

Your certificate must contain two parts:

- The private key used to encrypt information sent back to the client (file extension **.key**).
  - The server certificate (file extension **.crt**).
1. Put the **\*.key** file and the **\*.crt** file into a ZIP archive.
  2. Copy this ZIP file to a local directory that can be accessed by ARIS Cloud Controller (ACC).
  3. Start ARIS Cloud Controller (ACC) (page 2).
  4. Stop the **loadbalancer** runnable. Enter, for example: **stop loadbalancer\_m**
  5. Enter the ACC command **enhance loadbalancer\_<s, m, or l> with sslCertificate local file "<path to the ZIP file>"**

Example: **enhance loadbalancer\_m with sslCertificate local file "c:\\temp\\lbcert.zip"**.

If you have blanks or special characters in the path, you must put it in quotes and use a double backslash instead of a single slash. Alternatively, use single forward slashes, for example: **"c:/temp/lbcert.zip"**.

6. Start the **loadbalancer** runnable again. Enter, for example: **start loadbalancer\_m**

The SSL certificate is available.

If ARIS clients cannot perform connections to servers using TLS certification, you need to provide an additional certificate (see: **Basic Troubleshooting Guide**).

## 1.7.8 Redirect ports

In case of port conflicts (see **Basic Troubleshooting Guide**) redirect the ports, for example, the default HTTP port **80** or the HTTPS port **443**.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Run a **reconfigure** command on the **loadbalancer** runnable.

To make the **loadbalancer** runnable know through which ports users are now accessing it, you need to run an ACC **reconfigure** command with the following syntax:

**reconfigure loadbalancer\_<SIZING>**

**HTTPD.zookeeper.application.instance.http.port=<externalHttpPort>**

**HTTPD.zookeeper.application.instance.port=<externalHttpsPort>**

Replace **<SIZING>** with the sizing you used to install ARIS Server, such as **s**, **m**, or **l**.

Replace **<externalHttpPort>** with the port from which you redirect to the physical HTTP port of the **loadbalancer** runnable (usually port **80**).

Replace **<externalHttpsPort>** with the port from which you redirect to the physical HTTPS port of the **loadbalancer** runnable (usually port **443**).

This example tells the **loadbalancer** runnable in an **m** size installation that users are now accessing it through the redirected ports **80** and **443**:

**reconfigure loadbalancer\_m HTTPD.zookeeper.application.instance.http.port=80**

**HTTPD.zookeeper.application.instance.port=443**

ARIS users access ARIS using the redirected ports.

If runnables do not start up properly, resolve possible port conflicts.

## 1.7.9 Redirect HTTPS port

To make ARIS accessible under a privileged port on a Linux system, a user with root privileges has redirect the ports, for example, the HTTP port **80** or the HTTPS port **443**.

If you have forced the **loadbalancer** runnable to use HTTPS using an ACC command, such as:

```
reconfigure loadbalancer_m +HTTPD.EnforceHTTPS="true"
```

connections cannot be established. This is because users are forwarded to **https://<server name>:1443/** instead of **https://<server name>**.

You must redirect the HTTPS port to **443**.

### Procedure

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

```
reconfigure loadbalancer_m HTTPD.redirect.https.port=":443"
```

You must enter a colon followed by the port number.

Users are forwarded correctly.

## 1.7.10 Collect log files (ACC)

If problems occur during operation, you can use log files to find and resolve errors. You can download zipped log files related to each runnable or you can download all available log files.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To collect log files, for example related to the **abs\_I** runnable and save them in the specified directory, enter: **collect log files for abs\_I to C:\logfiles**

To collect all log files, enter: **collect log files** or **collect logfiles**

You can use additional parameters. To get information about the usage of ACC commands, enter **help** or **help <command>**.

All log files are stored as a ZIP archive.

If you cannot solve the problems and have a maintenance agreement, please send an error description and the ZIP archives containing collected log files as well as the entire contents of the **log** and **config** directories to the ARIS Global Support via Empower (<https://www.softwareag.com/corporate/services/support/default>).

## 1.7.11 Delete log files

Log files may contain private data of ARIS users, such as IP addresses, MAC addresses, or user names. In order to comply with the **General Data Protection Regulation (GDPR)**, you can collect log files using ACC or the ACC interface, find personal data related to deleted users, and manually delete or anonymize log file entries in source files.

### Warning

If you delete log files (page 22), Software AG might no longer be able to support you in order to resolve software problems.

In order to delete all log files, you must stop (page 16) the related runnables to allow unhindered access to all files. If you do not stop the runnables, some files may be locked and cannot be deleted.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To delete log files, for example related to the **abs\_I** runnable, enter: **delete log files for abs\_I**

To delete all log files, enter: **delete log files** or **delete logfiles**



All log files that are not accessed by a runnable are deleted. Log files that were not deleted are listed.

## 1.7.12 ARIS Administration/ARIS Risk and Compliance

If you have installed ARIS Risk and Compliance and ARIS Server you can force ARIS Risk and Compliance to use the ARIS Administration of the ARIS Server.

### 1.7.12.1 Specify a white list for ARIS Administration

You can specify a white list for ARIS Administration.

A white list or black list is a positive or negative list with which systems can be protected.

White lists and black lists pursue opposing strategies.

A white list contains all permitted URLs. A blacklist, on the other hand, specifically excludes URLs.

#### Procedure

1. Navigate to **<ARIS installation path>\server\bin\work\work\_umcadmin\_m**, for example, **C:\ARIS10.0\server\bin\work\work\_umcadmin\_m**.
2. Start ARIS Cloud Controller (ACC) (page 2).
3. Stop the ARIS Administration runnable. Enter, for example, **stop umcadmin\_<s, m, or l>**.
4. You must use regular expressions for the white list. A regular expression is a character string used to describe sets of character strings using certain syntactic rules.

Enter reconfigure **umcadmin\_<s, m, or l>**

**"JAVA-Dcom.aris.umc.whitelist.url.regex.pattern"="<comma-separated list of regular expressions>"**.

#### Example

If you want to allow a URL whose name consists of one word in lowercase letters and begins with **https://** and ends with **.com**, use the following regular expression:

**https://[a-z]+.com**

if you want to allow graphics of **jpg** typewhose names consist of mixed-case alphanumeric characters, and which are located in subdirectories of a URL that begins with **https://** and ends with **.com**, use the following regular expression:

**https://([a-z]\*.)[a-z]\*[.com](/[a-z]\*)/(/[a-z]\*)/([A-Za-z0-9\_]+.jpg)**

5. Start the ARIS Administration runnable. Enter, for example, **start umcadmin\_<s, m, or l>**.

You have specified a white list for ARIS Administration.

You can remove the white list again. To do so, proceed as described above and configure **reconfigure umcadmin\_m -"JAVA-Dcom.aris.umc.whitelist.url.regex.pattern"**.

## 1.7.12.2 Use existing ARIS document storage and ARIS Administration for ARIS Risk and Compliance

After you have installed ARIS Risk and Compliance this installation uses a separate set of runnables, for example, ARIS Administration or ARIS document storage. This means that the administrator has to manage users and documents. If you already use ARIS Server and have installed ARIS Risk and Compliance later you can reconfigure your ARIS Risk and Compliance runnable to your productive ARIS Server installation. This will make ARIS Risk and Compliance available to all users of your productive system and only one ARIS document storage will be in use.

1. Start ARIS Cloud Controller (ACC) (page 2).  
Make sure to start the ACC of your ARIS Risk and Compliance installation.
2. To reconfigure ARIS Risk and Compliance and force that runnable to use the ARIS Administration of your ARIS Server installation, enter: **reconfigure arcm\_<s,m or l> zookeeper.connect.string="<ARISServer>\\:14281"**

ARIS Risk and Compliance is now accessible via the ARIS Server name, for example, **http://arisserver/arcm** by all users managed within the ARIS Administration of your productive system.

To ensure more memory for the ARIS Risk and Compliance system you can shut down all other runnables or remove them.

## 1.7.13 Process Governance

For information on Process Governance customization, please refer to the **Process Governance Command-Line tool.PDF** and the **Process Governance Customizing. PDF**.

Where to find technical documents:

- ARIS installation package (...Documents\English\5 Customizing)
- Empower (<https://empower.softwareag.com/>)
- ARIS Download Center (<https://aris.softwareag.com/>)

## 1.7.14 ARIS Aware

You can make custom widgets available for ARIS Aware.

### 1.7.14.1 Make enhancements available

If you want to use self-designed widgets, **LESS** files, or **CSS** files in your ARIS Aware dashboards you must enhance each **dashboarding** runnable of your ARIS Server installation with these files. Enhanced files are not affected by an update setup. They will be preserved.

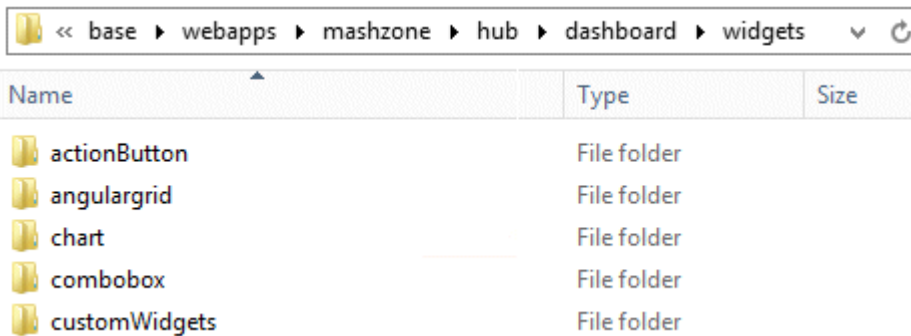
#### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To make the custom resource available enter, for example: **enhance dashboarding\_m with customResource local file "C:\\mywidgets.zip"**

If you have blanks or special characters in the path, you must put it in quotes and use a double backslash instead of a single slash.

The **ZIP** file including its contained folder structure is automatically extracted to the path:

**%INSTANCEDDIR%\\base\\webapps\\mashzone**



The screenshot shows a file explorer window with the address bar displaying the path: <code>base > webapps > mashzone > hub > dashboard > widgets</code>. Below the address bar is a table listing the contents of the 'widgets' folder.

Name	Type	Size
actionButton	File folder	
angulargrid	File folder	
chart	File folder	
combobox	File folder	
customWidgets	File folder	

## 1.7.15 ARIS Publisher

In this chapter product-related examples for configuring the system are available.

From ARIS 10.0.13.0 on ARIS Publisher and IT Inventory are no longer delivered. This means that you can no longer install or update ARIS Publisher Server. You can still use your current ARIS Publisher installation, but since this component is no longer supported, no more features will be developed. We strongly recommend using the ARIS portal (Published content) instead of ARIS Publisher in the future.

### 1.7.15.1 Provide ARIS Publisher license files

You can provide license files for ARIS Publisher Server using ACC. All other licenses are managed by ARIS Administration.

#### Procedure

1. Save the zip file to a local directory that can be accessed by ARIS Cloud Controller (ACC), for example: **d:/Publisher\_Server\_key.zip**
2. Start ARIS Cloud Controller (ACC) (page 2).
3. Stop the **businesspublisher** runnable. Enter, for example: **stop businesspublisher\_l**
4. Provide the license using this command: **enhance <runnable> with license local file <path to the saved file>**

Example: **enhance businesspublisher\_l with license local file "d:\\Publisher\_Server\_key.zip"**

If you have blanks or special characters in the path, you must put it in quotes and use a double backslash instead of a single slash. Alternatively, use single forward slashes, for example: **"d:/Publisher\_Server\_key.zip"**.

5. Start the **businesspublisher** runnable. Enter, for example: **start businesspublisher\_l**.

The license is available.

## 1.7.15.2 Reconfigure settings

You can change settings entered during the setup process. Use the **reconfigure** ACC command to change settings, such as ports (page 20). When performing an update setup all modifications made manually in CFG or XML files will be lost.

In this example, the connection parameters to Process Governance are adjusted.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Reconfigure **businesspublisher\_<s, m, or l>** and force that runnable to use the ARIS Administration of your ARIS Server installation.

Ensure that all values used in the **reconfigure** command, for example, for the keys **username** or **password** actually match to the values used in the <ARIS installation path>\server\bin\work\work\_businesspublisher\_<s, m or l>\base\webapps\businesspublisher\config\**webappserver.cfg** file and the **umcconfig.cfg** file. If typos were made during the setup process, the affected values must be adjusted.

For better readability, the parameters of the command are shown with line-wraps. For execution you must enter a single-line command.

```
bp.age.host="<aris-design-or-connect-srv>.domain.tld"
```

```
bp.age.port=80
```

3. For execution enter a single-line command. For better readability, the parameters of the reconfigure command are shown with line-wraps, for example:

```
reconfigure businesspublisher_<s, m, or l>
```

```
bp.ado.database="com.idsscheer.aris.businesspublisher.application.dao.database.AOracleDAO"
```

```
bp.db.driver="oracle.jdbc.OracleDriver"
```

```
bp.db.url="jdbc:oracle:thin:@//oracle-srv.domain.tld:1521:oracle_sid"
```

```
bp.db.validation.query="select 1 from dual"
```

```
bp.db.username="ARISBP"
```

```
bp.db.passwd="ARISBP"
```

```
bp.arisbpdata="ARISBPDATA"
```

```
bp.arisbpindex="ARISBPINDEX"
```

```
bp.login.module="UMCLogin"
```

```
bp.umc.server.url="http://<aris-design-srv>.domain.tld:<port number>/umc"
```

```
bp.umc.admin.login="superuser"
```

```
bp.umc.admin.passwd="<superuser's password>"
```

```
bp.age.host="<aris-design-srv>.domain.tld"
```

```
bp.age.port=80
```

This **businesspublisher\_<s, m, or l>** runnable is reconfigured. Publisher users are authenticated via ARIS Administration and ARIS document storage will be available if it has been connected to the ARIS Publisher Server.

These modifications will not be affected by update setups. When performing an update setup all modifications made manually in CFG or XML files will be lost.



### 1.7.15.3 Configure the service 'Create static ARIS Publisher export' for Process Governance

You can change settings entered during the setup process. Use the **reconfigure** ACC command to change settings, such as ports (page 20). When performing an update setup all modifications made manually in CFG or XML files will be lost. You can configure, that the **Create - Static ARIS Publisher export** service supports the port information.

#### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2) on your <\_apg\_server>.
2. Enter the following command, for example: **reconfigure apg\_m JAVA-Dcom.idsscheer.age.serviceenabling.staticExport.wsServer="<myARIShost>:<port>/aris/apgstatic"**

Ensure that all values used in the **reconfigure** command, for example, for the keys **username** or **password** actually match the values used in the <ARIS installation path>\server\bin\work\work\_apg\_<s, m or l>. If typing errors happened during the setup process the affected values must be adjusted.

This **apg\_m** runnable is reconfigured.

These modifications will not be affected by update setups. When performing an update setup all modifications made manually in CFG or XML files will be lost.

## 1.7.16 Collaboration

In this chapter related examples for configuring the system are available.

### 1.7.16.1 Specify a black list for Collaboration

You can specify a black list for Collaboration. Collaboration is the platform for cooperation across teams. With Collaboration, information can be exchanged faster, knowledge can be shared, and cooperation across borders is improved. Collaboration is a forum in which users can mention any URL in posts. It is therefore more appropriate to define a black list.

A white list or black list is a positive or negative list with which systems can be protected. White lists and black lists pursue opposing strategies.

A white list contains all permitted URLs. A blacklist, on the other hand, specifically excludes URLs.

#### Procedure

1. Navigate to **<ARIS installation path>\server\bin\work\work\_ebp\_<s, m, or l>**, for example, **C:\ARIS10.0\server\bin\work\work\_ebp\_m**.
2. Start ARIS Cloud Controller (ACC) (page 2).
3. Stop the Collaboration runnable. Enter, for example, **stop ebp\_<s, m, or l>**.
4. You must use regular expressions for the white list. A regular expression is a character string used to describe sets of character strings using certain syntactic rules.

Enter reconfigure **ebp\_<s, m, or l>**

**"JAVA-Dcom.aris.umc.blacklist.url.regex.pattern"="<comma-separated list of regular expressions>"**.

#### Example

If you want to block yahoo.com, use the following regular expression:

```
(http(s)?://)?([\w-]+\.)+[\w-]+[\\yahoo\\.com]+(/[?%&=]*)?
```

5. Start the Collaboration runnable. Enter, for example, **start ebp\_<s, m, or l>**.

You have specified a black list for ARIS Administration.

You can remove the black list again. To do so, proceed as described above and configure **reconfigure ebp\_m -"ebp.blacklist.url.regex.pattern"**.

## 1.7.16.2 Create synchronization user

The synchronization user serves technical purposes only. No function or license privileges are assigned to this user. The synchronization user is required for synchronization processes executed in the background of Collaboration, for example, to synchronize the user data between ARIS Administration and Collaboration.

The synchronization user is automatically generated for every newly created tenant. If the synchronization user is not available, the system user is used instead, provided that the default password of the **system** user was not changed. If the **system** user cannot be used, you must manually create the synchronization user using ARIS Cloud Controller. By default, the synchronization user name is **\_aris\_tech\_user\_ecp\_techuser**.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To create the synchronization user enter, for example:  
**enhance umcadmin\_m with createUser trigger only options tenant.name=<tenant name> tenant.user.name="<user name>" tenant.user.pwd="<user password>" affected.user="<synchronization user name>" affected.email="<synchronization user e-mail>" affected.pwd="<synchronization user password>" as.technical.user="true"**  
**set tenant default data for app umc ecpTechnicalUserName="<synchronization user name>" ecpTechnicalUserPassword="<synchronization user password>"**

The user is created and made available for the **ecp** runnable.

## 1.7.16.3 Anonymize Collaboration user

You can anonymize deleted Collaboration users according to GDPR.

### Prerequisites

The user was deleted in ARIS Administration.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To anonymize, for example, the deleted **y4711** user on **ecp\_m** enter: **invoke anonymizeUser on ecp\_m anonymize.user=y4711**

Activities of this Collaboration user, such as posts, comments, groups, are shown with **Anonymized user** instead with the **y4711** user name. If several users are anonymized a number is added, such as **Anonymized user 2**.

## 1.7.16.4 Force synchronize Collaboration users

You can transfer users managed in ARIS Administration to Collaboration. This can affect all users or list of users.

### Prerequisites

The user executing the command is then **system** user or has the **Collaboration administrator** function privilege.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To transfer all users from ARIS Administration, enter, for example: **invoke refreshUsers on ecp\_m tenant.id=tenant01**
3. To transfer a list of users, enter, for example: **invoke refreshUsers on ecp\_m tenant.id=tenant01 user.list="user1,user2,user39"**

The list of user names must be comma separated without blanks.

By default **system** user credentials are used. If you execute the command as a user holding the **Collaboration administrator** function privilege, you must specify your user credentials, such as:

```
invoke refreshUsers on ecp_m tenant.id=tenant01 tenant.user=<user name>  
tenant.user.pwd=<password>
```

or:

```
invoke refreshUsers on ecp_m tenant.id=tenant01 tenant.user=<user name>  
tenant.user.pwd=<password> user.list="user1,user2,user39"
```

Users managed in ARIS Administration are available in Collaboration.

## 1.7.17 Tenant Management

In this chapter related examples for configuring the system are available.

### 1.7.17.1 Create a tenant

After the installation of ARIS the **default** tenant is available. If you need additional tenants to provide different sets of databases, users, configurations or ARIS methods you can easily create tenants. If you are going to create additional tenants for ARIS10.0 to migrate data from ARIS 9.8.7 or later, make sure to use identical names in both ARIS versions. You can also create tenants using the ARIS Administration's command line tools or Tenant Management.

#### Prerequisites

- ARIS Server installation
- Users need the **User administrator** function privilege.
- If you use an external database system that was configured using the delivered database scripts (see ARIS Server Installation Guide), assign the tenants (page 48) to these schemes before running the command as described below.

#### Warning

For tenant names please only use up to 25 lowercase ASCII characters and numbers. The name must begin with a character. Special characters, such as \_ and characters, for example, in Chinese, Cyrillic or Arabic cannot be used.

#### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Enter: **create tenant <tenant name> username=<user name of a user holding the required privileges> password=<this user's password>**.

Example: **create tenant test01 master.tenant.user.name = admin  
master.tenant.user.pwd= tenantmanager123**

You can even change parameters for the new tenant. You must specify additional parameters in case you use an external database management system, for example (Oracle):


```
create tenant test01 database.admin.user="system"  
database.admin.password="manager" dbinstanceid="db0000000000"  
database.schema.tablespace.default="ARISDATA"  
database.schema.tablespace temporary="TEMP"  
database.schema.name=aris_test01"  
database.schema.password="*ARIS!1dm9n#yy"
```

The tenant **test01** will be created.

3. The administrator must import licenses, create users and user groups and assign privileges and licenses for the **test01** tenant.
4. Start a ARIS client and log in using this tenant. The system database will be created for that tenant.

The tenant is created and can be backed up (page 36).

### 1.7.17.2 Back up a tenant

You can back up tenant data (page 40) using the ARIS Cloud Controller (ACC). If you want to include the user statistics, the property **User statistics in backup** (**com.aris.umc.user.statistics.backup**) must be enabled in the configuration (see ARIS help: ARIS Administration >  Configuration > User management > Security > Advanced settings). Please note that no user can work on this tenant during the backup process.

#### Prerequisites

- ARIS Server installation
- Users need the following function privileges. The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

▪ Analysis administrator	▪ License administrator
▪ ARCM administrator	▪ Portal administrator
▪ Collaboration administrator	▪ Process Governance administrator
▪ Database administrator	▪ Server administrator
▪ Dashboard administrator	▪ Technical configuration administrator
▪ Document administrator	▪ User administrator

#### Warning

Do not store backup files in ARIS document storage.

Tenant data is fully backed up only if the user executing the commands has sufficient privileges for all components in every tenant and if all components were selected for the backup.

User administration audit events are not part of the tenant backup.

Extensions, for example, TLS/SSL certificates (page 19), SAP® Java Connector, and JDBC drivers (page 46), added using the **enhance** ACC command are not backed up.

To avoid data inconsistencies and possible data loss, you must not perform any of the following activities in parallel, neither manually nor scheduled:

- Deleting any Process Governance process instance, process version, or process
- Archiving Process Governance process instances
- Backup/restore tenant (containing Process Governance or ARIS document storage data)

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Enter: **backup tenant <tenant name> to <pathToBackUpFile> encryption.key <encryption password or encryption key> username=<user name of a user holding the required privileges>password=<this user's password>**

such as: **backup tenant default to "f:\\backupDefault.acbcrypt"**

**encryption.key=str3ngG3h31m username=y1234 password=managery1234.** If

values contain special characters, you must quote the strings and special characters. If a password for example is **User&12345**, you must enter **password="\User\&12345\"**

Make sure to save the backup file on external media, such as a NAS or file server. Notice the double backslashes. Alternatively, use a single forward slash. If no file name is specified, the file name is generated as for unencrypted files, but with the file extension **acbcrypt** instead of **acb**. The encryption password must be at least 8 characters long and contain at least 3 out of the 4 following character classes: lower-case letter, upper-case letter, digit, special character (such as any non-whitespace, non-letter, non-digit character).

The backup is started. The complete backup is written to one single **acb** archive file. If you encrypted the backup file, the file extension is **acbcrypt**.

If a tenant backup containing Process Governance data takes a long time to complete, Process Governance downtime is likely to be long. To reduce Process Governance downtime while the backup is in process, you can set the **Use snapshot-based backup mode** property in the Process Governance configuration. For details, refer to the ARIS online help (Manage ARIS > Set up Process Governance > Valuable information >What infrastructure properties are available?).

You can restore (page 39) this tenant using the related archive file. Using the **restore tenant** command will copy the content to an existing tenant. Process Governance backup archives greater than 2 GB might lead to insufficient TEMP space issue when restoring them into ARIS with Oracle back end. For such large backups, extend the temp tablespace size before restoring operation executed.

You can manage tenants also using the ARIS Administration's command line tools or Tenant Management tool.

### 1.7.17.3 Delete a tenant

If you delete a tenant all tenant information are lost:

- Databases
- User data (users, privileges and licenses)
- ARIS document storage data including all access rights
- Process Governance data
- Ad hoc analyses and queries

**Prerequisites**

- ARIS Server installation
- Users need the following function privileges. The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

▪ Analysis administrator	▪ License administrator
▪ ARCM administrator	▪ Portal administrator
▪ Collaboration administrator	▪ Process Governance administrator
▪ Database administrator	▪ Server administrator
▪ Dashboard administrator	▪ Technical configuration administrator
▪ Document administrator	▪ User administrator

**Warning**

If you delete a tenant all tenant information are lost.

**Procedure**

1. Back up (page 36) the tenant in order to be able to restore (page 39) data again.
2. Start ARIS Cloud Controller (ACC) (page 2).
3. Enter: **delete tenant <Tenant name> username=<user name of a user holding the required privileges> password=<this user's password>**

Deletes the specified tenant and all its associated data from the system. User name and password of an administrative user have to be specified using the parameters **master.tenant.user.name** and **master.tenant.user.pwd**, respectively. If values contain special characters, you must quote the strings and special characters. If a password for example is **User&12345**, you must enter **password=\"User\&12345\"**

**Warning**

If the optional **force** keyword is used, the security question **Are you sure?** is not displayed and the tenant and its data will be deleted without further prompting the user.

The tenant has been deleted.



You can also manage tenants using the ARIS Administration's command line tools or Tenant Management.

### 1.7.17.4 Restore a tenant

You can restore tenant data (page 40) or copy the content of this tenant (page 43) to a different ARIS server. You need to have access to the relevant back-up archive file containing the data of a tenant:

#### Warning

No user can work on this tenant during the restore process. All current data of a running tenant will be deleted and replaced by the data of the backup file. Data related to ARIS Administration will not be deleted but merged. The tenant name and current user data will be untouched. If users were deleted after the tenant has been backed up, these users will be available again. Make sure to delete those users.

Process Governance backup archives greater than 2 GB might lead to insufficient TEMP space issue when restoring them into ARIS with Oracle back end. For such large backups, extend the temp tablespace size before restoring operation executed.

To avoid data inconsistencies and possible data loss, you must not perform any of the following activities in parallel, neither manually nor scheduled:

- Deleting any Process Governance process instance, process version, or process
- Archiving Process Governance process instances
- Backup/restore tenant (containing Process Governance or ARIS document storage data)

#### Prerequisites

- You need access to the relevant back-up archive file.
- ARIS Server installation
- Users need the following function privileges. The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

▪ Analysis administrator	▪ License administrator
▪ ARCM administrator	▪ Portal administrator
▪ Collaboration administrator	▪ Process Governance administrator
▪ Database administrator	▪ Server administrator
▪ Dashboard administrator	▪ Technical configuration administrator
▪ Document administrator	▪ User administrator

## Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To restore the tenant, enter: **restore tenant <tenant name> from <pathToBackUpFile> encryption.key <encryption password or encryption key> username=<user name of a user holding the required privileges> password=<this user's password>**

such as: **restore tenant default from "f:\\backupDefault.acbcrypt" encryption.key=str3ngG3h31m username=y1234 password=managery1234**

or as an example for the use of an unencrypted **acb** file: **restore tenant default from "f:\\backupDefault.acb" username=y1234 password=managery1234**

Notice the double backslashes. Alternatively, use a single forward slash. If values contain special characters, you must quote the strings and special characters. If a password for example is **User&12345**, you must enter **password="\User\&12345\"**

The tenant will be restored.

3. Make sure to change the standard user's passwords again.

The tenant is restored. You can also manage tenants using the Tenant Management tool or the ARIS Administration's command line tools.

If you have restored a tenant from an ARIS 10 SR5 backup file or earlier containing ARIS document storage data, you must adjust the timestamps manually (page 45) (see **y-admintool.bat** command-line tool).

### 1.7.17.5 What data is backed up and restored?


If you back up tenants, the current state of the following data is saved in different folders in the tenant backup zip file.

Tenant data is fully backed up only if the user executing the commands has sufficient privileges for all components in every tenant and if all components were selected for the backup. In ARIS 10 all started runnables are automatically taken into account when executing tenant backup/restore commands.

#### Warning

To avoid data inconsistencies and possible data loss, you must not perform any of the following activities in parallel, neither manually nor scheduled:

- Deleting any Process Governance process instance, process version, or process
- Archiving Process Governance process instances
- Backup/restore tenant (containing Process Governance or ARIS document storage data)

Content	Required function privileges	Component (runnable)
<p>Data from ARIS Administration, for example, users, privileges.</p> <p>User statistics are not included by default. If you want to include the user statistics, the property <b>User statistics in backup (com.aris.umc.user.statistics.backup)</b> must be enabled in the configuration (see ARIS help: ARIS Administration &gt;  Configuration &gt; User management &gt; Security &gt; Advanced settings).</p>	<p>User administrator</p> <p>Technical configuration administrator</p>	<p>ARIS Administration/User Management</p> <p>(umcadmin_&lt;s, m, or l&gt;)</p>
<p>Licenses</p> <p>User administration audit events are not part of the tenant backup.</p>	<p>License administrator</p>	
<p>System database</p> <p>Contains filters, templates, and font formats, but also ARIS Method and all evaluation scripts, macros and scheduled reports.</p>	<p>Server administrator</p>	<p>Modeling &amp; Publishing</p> <p>(abs_&lt;s, m, or l&gt;)</p>
<p>ARIS databases</p>	<p>Database administrator</p>	
<p>Ad hoc analyses and queries</p>	<p>Analysis administrator</p>	<p>Analysis</p> <p>(octopus_&lt;s, m, or l&gt;)</p>
<p>ARIS document storage data, including Process Governance archives</p> <p>Documents and access privileges</p>	<p>Document administrator</p> <p>Technical configuration administrator</p>	<p>ARIS document storage</p> <p>(adsadmin_&lt;s, m, or l&gt;)</p>

Content	Required function privileges	Component (runnable)
Process Governance data	Process Governance administrator	Process Governance (apg_<s, m, or l>)
Collaboration data	Collaboration administrator	Collaboration (ecp_<s, m, or l>)
ARIS Risk and Compliance data	ARCM administrator	ARIS Risk and Compliance (arcm_<s, m, or l>)
Dashboards and feeds	Dashboard administrator	ARIS Aware (dashboarding_<s, m, or l>)
ARIS portal views, modification sets, and configuration sets.	Portal administrator	ARIS portal (copernicus_<s, m, or l>)

## 1.7.17.6 Copy a tenant to a different server

You can copy the content of a backed up tenant to a different ARIS Server. This procedure can also be used to migrate data in case of an upgrade installation. You need to have access to the relevant back-up archive file containing the data of a tenant:

- All databases
- All user data (users, privileges and licenses)
- All ARIS document storage data including all access rights
- All Process Governance data
- All ad hoc analyses and queries

Extensions, for example, TLS/SSL certificates (page 19), SAP® Java Connector, and JDBC drivers (page 46), added using the **enhance** ACC command are not backed up.

### Prerequisites

- You need access to the relevant back-up zip file
- ARIS Server installation
- Users need the following function privileges. The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

▪ Analysis administrator	▪ License administrator
▪ ARCM administrator	▪ Portal administrator
▪ Collaboration administrator	▪ Process Governance administrator
▪ Database administrator	▪ Server administrator
▪ Dashboard administrator	▪ Technical configuration administrator
▪ Document administrator	▪ User administrator

### Procedure

1. Create a tenant (page 35) on the ARIS Server where the tenant will be copied to and import the licenses.
2. Start ARIS Cloud Controller (ACC) (page 2).
3. To restore Process Governance data, stop the Process Governance runnable first. To do so enter, for example: **stop apg\_m**

4. Enter: **restore tenant <Tenant name> from <pathToBackupFile> encryption.key <encryption password or encryption key> username=<user name of a user holding the required privileges> password=<this user's password>**

or as an example for the use of an unencrypted **acb** file: **restore tenant default from "f:\\backupDefault.acb" username=y1234 password=managery1234**

Notice the double backslashes. Alternatively, use a single forward slash. If values contain special characters, you must quote the strings and special characters. If a password for example is **User&12345**, you must enter **password="User\&12345"**. You must enter the user credentials of the server's ARIS Administration you have created the new tenant. If you are about to migrate data, you might use the standard name and password **system/manager**.

5. In case you restored Process Governance data, restart the Process Governance runnable. To do so enter, for example: **start apg\_m**

All data of the backup file will be copied to the new tenant. Current data will be deleted except the name of the new tenant, as well as user credentials. The current user data will be untouched. If users were deleted after the tenant has been backed up, these users will be available again. Please make sure to delete those users.

In case of a migration process the default credentials will automatically be in use. To prevent unauthorized access to the ARIS system, after installation or data migration, always change the default passwords of all users that are automatically created (**arisservice** user, **guest** user, **system** user, **superuser** user) on all operational tenants, as well as on the infrastructure tenant (master).

You can also create tenants using the ARIS Administration's command line tools or Tenant Management.

## 1.7.17.7 How to adjust timestamps related to ARIS document storage

In previous ARIS versions, ARIS document storage stored timestamps, for example **Creation time** and **Update time**, referred to documents and folders in local server time and without any time zone information. If data was moved between ARIS Servers or if a tenant was restored from a backup file, timestamps were likely adjusted using a wrong time offset.

Since ARIS 10 SR6, **Coordinated Universal Time** (UTC) is mandatory for timestamps stored by ARIS document storage. Because time zone information in existing data is not available, the timestamps of existing documents and folders cannot be adjusted automatically. After the update to ARIS 10 SR6, you must manually adjust timestamps. In a Windows-based installation with local time UTC-2, for example, use the **y-admintool.bat** command-line tool and, considering UTC offset of your ARIS Servers>, enter the following:

```
y-admintool.bat -s https://localhost -t default adjustTimestamps -offset "-120" -u system -p manager
```

If you have restored a tenant from backup file created with ARIS 10 SR5 or earlier, you must adjust the timestamps as well.

## 1.7.18 Database connection

This chapter provides information on configuring ARIS Server in order to use an external database management system.

### 1.7.18.1 Provide JDBC drivers

During the setup procedures of ARIS Server or ARIS Publisher Server using Oracle or Microsoft SQL Server the JDBC driver is provided automatically. You can enhance JDBC drivers manually.

#### Procedure

1. Download the JDBC driver from the Microsoft or Oracle Web Sites to local directory that can be accessed by ARIS Cloud Controller (ACC).  
For example: **d:\ojdbc<number>.jar**.
2. Start ARIS Cloud Controller (ACC) (page 2).
3. Stop the server runnables. Enter: **stopall**.
4. Provide the JDBC driver using the **enhance** command. If you have blanks or special characters in the path, you must put it in quotes and use a double backslash instead of a single slash.
5. Example: **enhance abs\_I with webappsClasspath local file "d:\\ojdbc<number>.jar"**  
The file is copied to the <ARIS installation directory>\server\bin\work\work\_abs\_I\base\lib. The source file can be deleted.
6. Delete obsolete JDBC driver files from the <ARIS installation directory>\server\bin\work\work\_abs\_I\base\lib. If you add the latest file to update your JDBC driver with the **enhance** ACC command, both driver files, the obsolete file and the latest file are present. As a result, runnables will not start correctly because the JDBC driver to be used cannot be determined.
7. Start the server runnables. Enter: **startall**

The driver is available.



## 1.7.18.2 Update external service (database clusters)

If you have performed an installation using an Oracle or Microsoft SQL database cluster you need to reconfigure the external service after the installation process.

This procedure shows an example for an Oracle database.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To connect to an Oracle cluster using a JDBC URL you may use this example:

```
update external service <dbserviceID>  
url="jdbc:oracle:thin:@(DESCRIPTION=ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP  
) (HOST=<virtual-ip-oracle-cluster>)(PORT = <target  
port>)))(CONNECT_DATA=(SERVICE_NAME=cluster-database-name))"  
driverClassName="oracle.jdbc.OracleDriver" username="<cip_app_user>"  
password="<new_cip_app_pwd>" maxIdle=15 maxActive=100 maxWait=10000  
removeAbandoned=false removeAbandonedTimeout=600 logAbandoned=true  
defaultAutoCommit=false rollbackOnReturn=true host=<target_host>  
jmxEnabled=true validationQuery="select 1 from dual" testOnBorrow=true
```

ARIS Server can be started using the Oracle cluster.

### 1.7.18.3 Configure the database connection for additional schemes

#### ASSIGN TENANT TO DATABASE SCHEMA

During the setup process you have created an empty Oracle or Microsoft SQL schema for an additional tenant (see ARIS Server Installation Guide). Additionally created tenants must be assigned to the database schema. Replace values in angle brackets, such as **<tenant name>** with your own values, such as new **tenant1**.

1. Start ARIS Cloud Controller (ACC) (page 2).
2. To discover the database service ID (<dbserviceID>, such as db000000000), enter:

**list external services**

```
assign tenant <tenant name> to service <dbserviceID> com.aris.cip.db.schema =<schema name>
```

For tenant names please only use up to 25 lowercase ASCII characters and numbers. The name must begin with a character. Special characters, such as \_ and characters, for example, in Chinese, Cyrillic or Arabic cannot be used.

3. To create a new tenant, enter:

**create tenant <tenant name>**

The new tenant is available on ARIS Server.

#### ADDITIONAL SETTINGS

To enable **validationQuery** for external database connections (Oracle & Microsoft SQL) please use the correct validation query for the DBMS.

**For Oracle use:**

```
validationQuery="select 1 from dual" and testOnBorrow=true
```

**For Microsoft SQL use:**

```
validationQuery="select 1" and testOnBorrow=true
```

For better readability, the parameters of the command are shown with line-wraps. For execution you must enter a single-line command.

During registration of external service add parameters, for example, for Oracle:

```
register external service db
url="jdbc:oracle:thin:@<target_host>:<target_port>:<oracle_sid>"
driverClassName="oracle.jdbc.OracleDriver"
username="<cip_app_user>"
password="<cip_app_pwd>"
maxIdle=15
maxActive=100
maxWait=10000
removeAbandoned=false
removeAbandonedTimeout=600
defaultAutoCommit=false
rollbackOnReturn=true
host=<target_host>
port=<target_port>
jmxEnabled=true
validationQuery="select 1 from dual"
testOnBorrow="true"
```

After the external service was already registered, for example, for Oracle:

```
update external service <dbserviceID>
url="jdbc:oracle:thin:@<target_host>:<target_port>:<oracle_sid>"
driverClassName="oracle.jdbc.OracleDriver"
username="<cip_app_user>"
password="<cip_app_pwd>"
maxIdle=15
maxActive=100
maxWait=10000
removeAbandoned=false
removeAbandonedTimeout=600
defaultAutoCommit=false
rollbackOnReturn=true
host=<target_host>
jmxEnabled=true
validationQuery="select 1 from dual"
testOnBorrow="true"
```

### ENABLE VALIDATIONQUERY FOR EXTERNAL POSTGRESQL CONNECTION

1. Enter: **stopall**
2. Enter: **reconfigure <postgres\_runnable> dbsp.validationQuery="select 1"  
dbsp.testOnBurrow=true**
3. Enter: **startall**

The database connection is configured.

## 1.7.18.4 Move the database management system

If you run ARIS using an external database management system and the operational database server has moved, you must update the settings, for example, the IP address and the server name.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Stop all runnables, except the **zoo** runnable (service registry).
3. Determine the service ID of the external database service to be changed. Enter: **list external services**
4. Check the current settings of the external database settings. Enter: **show external service <service ID>**

Example: **show external service db0000000000**

Depending on the database system in use different settings are displayed.

#### Output example (Oracle):

Service db0000000000 (Type DB)

Parameters:

...

host sbrva100.com.ad.aaf

...

url jdbc:oracle:thin:@//sbrva100.com.ad.aaf:1521/aris

...

#### Output example (Microsoft SQL Server):

Service db0000000000 (Type DB)

Parameters:

...

host sbrva100.com.ad.aaf

...

url jdbc:sqlserver://sbrva100.com.ad.aaf;DatabaseName=aris10db;instanceName=aris

...

5. Change the required settings using the **update external service** command.

**Example (Oracle):**

```
update external service <service ID> url="jdbc:oracle:thin:@//<Oracle server>:<listener port>/<instance name>" host=<Oracle server>
```

**Example (Microsoft SQL Server):**

```
update external service <service ID> url="jdbc:sqlserver://<Microsoft SQL Server>:<listener port>;DatabaseName=<database name>;instanceName=<instance name>" host=<Microsoft SQL Server>
```

6. Check the applied database schema. Enter: **list tenant <name> data for service db**

**Output example (default tenant):**

```
Data of tenant default tenant for application db
Key Value
com.aris.cip.db.schema aris_default
com.aris.ecp.db.schema aris_default
name default
```

7. Change the schema settings for all tenants, if required. Enter:

```
set tenant <tenant name> data for service db com.aris.cip.db.schema=<new schema name>
```

**Example (master tenant):**

```
set tenant master data for service db com.aris.cip.db.schema=aris10_master (com.aris.ecp.db.schema not needed)
```

**Example (default tenant):**

```
set tenant default data for service db com.aris.cip.db.schema=aris10_default com.aris.ecp.db.schema=aris10_default
```

8. Check the new settings using the commands:

```
show external service <service ID>
```

```
list tenant <tenant name> data for service db
```

9. Start all runnables. Enter: **startall**

## 1.7.19 Elasticsearch

The Document index (Elasticsearch) is a basic component that contains the full-text search index for documents and collaboration data. It also stores users, user groups, licenses, and privileges. By default, the **elastic\_<s, m, or l>** runnable (Elasticsearch) uses generic user credentials required for communication with other ARIS runnables.

### 1.7.19.1 Check user name and password (Elasticsearch)

By default, the **elastic\_<s, m, or l>** runnable (Elasticsearch) uses generic user credentials required for communication with other ARIS runnables. You can check the user name and password in use.

#### Procedure

1. Navigate to **<ARIS installation path>\server\bin\work\work\_elastic\_m**, for example, **C:\ARIS10.0\server\bin\work\work\_elastic\_m**.
2. Open the **instanceld.elasticsearch** file with a text editor.
3. Copy the instance ID, for example:  
**elasticsearch0000000000**
4. Start ARIS Cloud Controller (ACC) (page 2).
5. Once ACC is initialized, enter **show service elastisearch<ID>**, for example:  
**show service elasticsearch0000000000**

User name and password are displayed.

```
ACC+ localhost>show service elasticsearch0000000000
Service elasticsearch0000000000 (Type ELASTICSEARCH)
Parameters:
Key      Value
ajpPort  8009
context  /
host     daetstdocu02.eur.ad.sag
password ngCIolG6rcysQksQwWlhnsGpVmLQubej
port     14220
scheme   http
username aris
```

You can change (page 53) the user name and the password if required.

## 1.7.19.2 Change user name and password (Elasticsearch)

By default, the **elastic\_<s, m, or l>** runnable (Elasticsearch) uses generic user credentials required for communication with other ARIS runnables. You can check (page 52) and change the user name and the password if required.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Once ACC is initialized, enter:  
**reconfigure elastic\_<s, m, or l> +ELASTICSEARCH.aris.api.user.name="<new user name> +ELASTICSEARCH.aris.api.user.password="<new password>"**

for example:

```
reconfigure elastic_m +ELASTICSEARCH.aris.api.user.name="administrator"  
+ELASTICSEARCH.aris.api.user.password="Thssmynwpsswr"
```

3. Stop the Collaboration runnable **eCP\_<s, m, or l>**. Enter, for example:  
**stop ecp\_m**
4. Restart the Collaboration runnable. Enter, for example:
5. **start ecp\_m**

You have changed the user credentials required for the Elasticsearch.

## 1.7.19.3 Disable authentication for Elasticsearch

You can switch off the authentication for the Elasticsearch.

### Warning

Disabling authentication is not recommended and must be considered carefully. It bears a potentially risk to data security.

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Once ACC is initialized, enter: **reconfigure elastic\_<s, m, or l> +ELASTICSEARCH.aris.api.deactivate.authentication="true"**

for example: **reconfigure elastic\_m**

```
+ELASTICSEARCH.aris.api.deactivate.authentication="true"
```

You have disabled the authentication for the Elasticsearch.





## 1.7.20.2 Monitor runnable's health

The **health** command determines a variety of health values for each runnable.

The exact list of health values available depends on the specific runnable. However, a few basic measurements are available to all runnables, in particular the CPU load and its memory usage. For all Java-based runnables, additional information is available.

### Prerequisite

Health monitoring parameters are set (page 56).

### Procedure

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Make sure that the runnable has been started.
3. Enter, for example: **show instance zoo\_m health**

The output will look like this example:

```
Status: OK
Specified IP or host name: arissrv
Resolved IP or host name: arissrv/127.0.0.1
Agent port: 9001
Monitored Resource      Current Value  Value Range   Low Thrh.    High Thrh.   State  Last merd. at  Merd. evry
CPU Load                11,36%        0,00%-100,00% 0,00%        80,00%       OK     08:05:39.844  1s 000ms
Memory Usage (Percent)  36,81%        0,00%-100,00% 0,00%        80,00%       OK     08:05:39.844  1s 000ms
Memory Usage (Megabytes) 2980MB        0MB-8097MB    0MB          0MB          OK     08:05:39.844  1s 000ms
Free Disk Space (Percent) 63,40%        0,00%-100,00% 3,00%        0,00%       OK     08:05:39.845  1s 000ms
Free Disk Space (Megabytes) 302361MB     0MB-476938MB 1000MB       0MB          OK     08:05:39.846  1s 000ms
Known used ports:
  Port  Runnable  Port Parameter
  2181  zoo_m     clientPort
  9001  (AGENT)   rest.port     DEFAULT
ACC+ arissrv>
```

The first column shows the name of the measured value and its physical unit, for example, megabytes, percent, etc.

The second column shows the current value of the health value. Note that this is not measured the moment the command is executed. The agent plugin will take measurements periodically, and this column will show the result of the last measurement.

The third column shows the range of possible values, for example, minimum and maximum value. If no minimum or maximum value can be determined or the value does not have an ordinal value scale a - is shown instead.

The fourth and fifth columns show the minimum and maximum values, respectively. These values were observed since the runnable or the ARIS Agent had last been restarted, but only if the health value measured has an ordinal value scale. For values measured without an ordinal value scale, - will be shown.

The sixth column shows the low or high warning thresholds for the measured value, if the measured health value has an ordinal value scale and if thresholds have been configured.

The seventh column shows the state of the measured value if the measured health value has an ordinal value scale and if a low and/or high threshold has been configured. The state can be either **OK**, **LOW** or **HIGH**. If in **LOW** or **HIGH** state, the column will also show for how long the value has been in that state already.

### 1.7.20.3 Configure health monitoring

If you use the health monitoring, using ACC, make sure to configure the system.

**Procedure**

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Enter the parameters described below.

#### THRESHOLDS

Thresholds for monitored values can be configured using agent configuration parameters:

Parameter	Description
<b>monitoring.high.cpu.threshold.percent</b> (0.0 – 1.0, default 0.8)	High CPU usage threshold (relative, in percent)
<b>monitoring.relative.low.disk.space.warning.threshold.percent</b> (0.0 – 1.0, default 0.03)	Low memory threshold (relative, in percent)
<b>monitoring.absolute.low.disk.space.warning.threshold.megabytes</b> (default 1000)	Low disk space threshold (absolute, in megabytes)
	<p><b>Warning</b></p> <p>ARIS Agent not only warns against insufficient disk space. When the default value (1000 MB) is reached, all runnables are immediately shut down (killall) to avoid data inconsistencies. Runnables cannot be restarted. ARIS Agent autostart is disabled.</p>

## THRESHOLD MEASUREMENT

The measurement can be configured by the following parameters:

Parameter	Description
<b>monitoring.interval</b> (default 1000)	Interval in milliseconds, in which the measurement will be done.
<b>monitoring.high.cpu.number.of.intervals.warning.threshold</b> (default 10)	Number of measurements with CPU load above threshold before a warning state is reached
<b>monitoring.high.mem.usage.number.of.intervals.warning.threshold</b> (default 10)	Number of measurements with memory usage above threshold before a warning state is reached.
<b>monitoring.low.disk.space.number.of.intervals.warning.threshold</b> (default 10)	Number of measurements with free disk space below threshold before a warning state is reached.

## MAIL NOTIFICATION

Mail notification can be configured by the following parameters:

Parameter	Description
<b>mail.notification.enabled</b> (default: <b>false</b> )	<b>true</b> enables automatic mailing.
<b>mail.smtp.host</b>	Qualified hostname or IP of the mail server.
<b>mail.smtp.port</b> (common: <b>25</b> )	Port of the mail server.
<b>mail.smtp.username</b>	User name on the mail server. If this parameter is set, the applications will implicitly enable SMTP authentication. There is <b>NO</b> dedicated parameter to explicitly enable SMTP authentication.
<b>mail.smtp.password</b>	Mail server password for the specified user.
<b>mail.sender.address</b>	Sender's e-mail address.
<b>mail.sender.name</b>	Sender's name.

Parameter	Description
<b>mail.recipients</b>	<p>Recipient's e-mail address.</p> <p>This parameter is multivalued, specify several recipients separated with commas, for example:</p> <p><b>set mail.recipients = "a@abc.com","b@abc.com"</b></p>
<b>mail.recipients.cc</b>	<p>Recipient's e-mail address (<b>C</b>arbon <b>C</b>opy(CC)).</p> <p>This parameter is multivalued (see <b>mail.recipients</b>)</p>
<b>mail.on.system.events</b>	<p>Defining events triggering e-mail notification.</p> <p>This parameter is multivalued, specify several event types separated by comma, for example:</p> <p><b>set mail.on.system.events =</b> <b>MACHINE_STATE_CPU_LOAD_HIGH, MACHINE_STATE_</b></p> <p>Possible values:</p> <ul style="list-style-type: none"><li>▪ MACHINE_STATE_LOW_DISK_SPACE_PERCENT</li><li>▪ MACHINE_STATE_OK_DISK_SPACE_PERCENT</li><li>▪ MACHINE_STATE_LOW_DISK_SPACE</li><li>▪ MACHINE_STATE_OK_DISK_SPACE</li><li>▪ MACHINE_STATE_CPU_LOAD_HIGH</li><li>▪ MACHINE_STATE_CPU_LOAD_OK</li><li>▪ MACHINE_STATE_MEMORY_USAGE_HIGH</li><li>▪ MACHINE_STATE_MEMORY_USAGE_OK</li></ul>

## 1.7.21 Mailing

This chapter provides information on configuring automatic mailing.

### 1.7.21.1 Configure ARIS Agent mail server connection

If only ARIS Agent is installed but no ARIS server you can activate automatic mailing in order to receive technical information from ARIS Agent. This will inform administrators, for example, about performance problems concerning ARIS Agent.

1. Start ARIS Cloud Controller (ACC) (page 2) on the machine where ARIS Agent is installed.
2. Enter the following lines one after the other.

Example:

```
set mail.notification.enabled=true
set mail.smtp.host=mailserver.us
set mail.smtp.port=25
set mail.smtp.username=<user name>
set mail.smtp.password=<password>
set mail.recipients=aris.administrator1@company.com
set mail.recipients.cc=aris.administrator2@company.com
set mail.sender.address=<COMPUTERNAME>@us.co
```

ARIS Agent mail server connection is set.

Mail notification can be configured by the following parameters:

Parameter	Description
<b>mail.notification.enabled</b> (default: <b>false</b> )	<b>true</b> enables automatic mailing.
<b>mail.smtp.host</b>	Qualified hostname or IP of the mail server.
<b>mail.smtp.port</b> (common: <b>25</b> )	Port of the mail server.
<b>mail.smtp.username</b>	User name on the mail server. If this parameter is set, the applications will implicitly enable SMTP authentication. There is <b>NO</b> dedicated parameter to explicitly enable SMTP authentication.

Parameter	Description
<b>mail.smtp.password</b>	Mail server password for the specified user.
<b>mail.sender.address</b>	Sender's e-mail address.
<b>mail.sender.name</b>	Sender's name.
<b>mail.recipients</b>	<p>Recipient's e-mail address.</p> <p>This parameter is multivalued, specify several recipients separated with commas, for example:</p> <p><b>set mail.recipients = "a@abc.com","b@abc.com"</b></p>
<b>mail.recipients.cc</b>	<p>Recipient's e-mail address (<b>C</b>arbon <b>C</b>opy(<b>CC</b>)).</p> <p>This parameter is multivalued (see <b>mail.recipients</b>)</p>
<b>mail.on.system.events</b>	<p>Defining events triggering e-mail notification.</p> <p>This parameter is multivalued, specify several event types separated by comma, for example:</p> <p><b>set mail.on.system.events =</b>  <b>MACHINE_STATE_CPU_LOAD_HIGH, MACHINE_STATE_</b></p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>▪ MACHINE_STATE_LOW_DISK_SPACE_PERCENT</li> <li>▪ MACHINE_STATE_OK_DISK_SPACE_PERCENT</li> <li>▪ MACHINE_STATE_LOW_DISK_SPACE</li> <li>▪ MACHINE_STATE_OK_DISK_SPACE</li> <li>▪ MACHINE_STATE_CPU_LOAD_HIGH</li> <li>▪ MACHINE_STATE_CPU_LOAD_OK</li> <li>▪ MACHINE_STATE_MEMORY_USAGE_HIGH</li> <li>▪ MACHINE_STATE_MEMORY_USAGE_OK</li> </ul>
<b>mail.on.state.change</b> (default: <b>FAILED</b> )	<p>Defining events triggering e-mail notification if a runnable is in the state <b>FAILED</b>.</p>

Parameter	Description
<b>mail.on.runnable.monitoring.events</b>	<p>Defining events triggering e-mail notification.</p> <p>This parameter is multivalued (see <b>mail.on.system.events</b>).</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>▪ RUNNABLE_MONITORING_HIGH_THRESHOLD_EXCEEDED</li> <li>▪ RUNNABLE_MONITORING_LOW_THRESHOLD_EXCEEDED</li> </ul>

### 1.7.21.2 Configure SMTP mail server connection

If you did not enter the SMTP server connection parameters during the setup process of a previous ARIS version you need to register your SMTP server manually.

1. Start ARIS Cloud Controller (ACC) (page 2).
2. Enter, for example:  
**register external service smtp host="YourMailServerAddressWithDomain" port=25**
3. Check that setting entering:  
**list external services**

SMTP mail server configuration is set.

You can modify SMTP configuration parameters using the **update external service** command.

Parameter	Type	Default value	Description
<b>Host</b> host	String		Qualified hostname or IP of the SMTP server.
<b>Port</b> port	Integer	25	Port of the SMTP server.
<b>User name</b> username	String		User name on the SMTP server. If this parameter is set, the applications will implicitly enable SMTP authentication. There is <b>NO</b> dedicated parameter to explicitly enable SMTP authentication.

Parameter	Type	Default value	Description
<b>Password</b> password	String		Password for the user on the SMTP server.
<b>Sender address</b> sender.address	String		Sender's e-mail address.
<b>TLS</b> use.tls	Boolean	false	Specifies if SMTP server is TLS enabled.
<b>TLS mode</b> tls.mode	String	STARTTLS S	Specifies the method used to secure the connection. Accepted values are <b>STARTTLS</b> and <b>SSL</b> . STARTTLS upgrades an initially insecure connection to an encrypted one without requiring a dedicated port for secure communication, whereas SSL immediately establishes a secured connection on a dedicated port.



## 1.7.22 Third-party document management systems (TDMS)

This chapter provides information on configuring ARIS Server to use an external TDMS.

### 1.7.22.1 Make TDMS available

If you want to use third-party document management systems, you must enhance the ARIS document storage runnable with a custom jar file. The systems available are **ARIS Adapter for Microsoft® SharePoint 2016** and **ARIS Adapter for Microsoft® SharePoint 2019**. Please contact your local Software AG sales organization (<http://www.softwareag.com>) for other third-party document management systems.

#### Procedure

1. Save the custom jar file for the third-party document management system.
2. Start ARIS Cloud Controller (ACC) (page 2).
3. Stop the ARIS document storage runnable. Enter, for example: **stop adsadmin\_m**
4. Provide the custom jar file for the third-party document management system using the **enhance** command. If you have blanks or special characters in the path, you must put it in quotes and use a double backslash instead of a single slash.

Example: **enhance adsadmin\_m with webappsClasspath local file "d:\\dms-adapter.jar"**

The file has been made available. The source file can be deleted.

5. Start the ARIS document storage runnable. Enter: **start adsadmin\_m**

The third-party document management system is available.

You must configure the settings for the TDMS in ARIS Administration, refer to chapter **Manage ARIS > Configure ARIS > Set up Document storage > Add third-party document management system** of the ARIS online help.

## 2 Legal information

### 2.1 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.

### 2.2 Support

If you have any questions on specific installations that you cannot perform yourself, contact your local Software AG sales organization (<https://www.softwareag.com/corporate/company/global/offices/default.html>). To get detailed information and support, use our websites.

If you have a valid support contract, you can contact **Global Support ARIS** at: **+800 ARISHELP**. If this number is not supported by your telephone provider, please refer to our Global Support Contact Directory.

## ARIS COMMUNITY

Find information, expert articles, issue resolution, videos, and communication with other ARIS users. If you do not yet have an account, register at ARIS Community.

## PRODUCT DOCUMENTATION

You can find the product documentation on our documentation website.

In addition, you can also access the cloud product documentation. Navigate to the desired product and then, depending on your solution, go to **Developer Center**, **User Center** or **Documentation**.

## PRODUCT TRAINING

You can find helpful product training material on our Learning Portal.

## TECH COMMUNITY

You can collaborate with Software AG experts on our Tech Community website. From here you can, for example:

- Browse through our vast knowledge base.
- Ask questions and find answers in our discussion forums.
- Get the latest Software AG news and announcements.
- Explore our communities.
- Go to our public GitHub and Docker repositories and discover additional Software AG resources.

## PRODUCT SUPPORT

Support for Software AG products is provided to licensed customers via our Empower Portal (<https://empower.softwareag.com/>). Many services on this portal require that you have an account. If you do not yet have one, you can request it. Once you have an account, you can, for example:

- Download products, updates and fixes.
- Add product feature requests.
- Search the Knowledge Center for technical information and tips.
- Subscribe to early warnings and critical alerts.
- Open and update support incidents.