ARIS
DATA PROTECTION (GDPR)

VERSION 10.0 - SERVICE RELEASE 8

April 2019

Document contentnot changed since release 10.0.6. It applies to the current version without changes.

Contents

1 Personal data used in ARIS products

In order to comply with the **G**eneral **D**ata **P**rotection **R**egulation (GDPR (page 17)), ARIS provides tools for anonymizing deleted users. The sections below explain:

- Which ARIS components save information, such as IP addresses, MAC addresses, user names, and images.
- How to delete personal data in ARIS (page 5).

1.1 ARIS Administration

User data are centrally managed in the User Management of the ARIS Administration. When creating users manually, the following data are mandatory:

- User name
- First name
- Last name

If users imported or synchronized using LDAP, additional personal data can be stored:

- E-mail address
- Telephone number
- LDAP DN
- ID
- Picture

User Management creates audit logs in databases. This provides a history of changes in function, license and access rights. For this purpose, user names and IP addresses are logged.

Even if users were deleted (page 6), user names are stored in an invisible attribute together with the time of deletion in order to log the changes. These invisible attributes are automatically deleted during an upgrade to a new major ARIS version. These entries can be anonymized (page 7) for deleted users.

1.2 ARIS databases

User names are stored for several purposes for different ARIS components. Even if a user is deleted in the User Management of the ARIS Administration (page 6), in ARIS databases the user name stays visible in the **Creator** and the **Last modifier** model and object attributes, and in change list descriptions. This also applies to archived models and objects. These entries can be anonymized (page 8).

1.3 ARIS document storage

ARIS document storage stores user names for several purposes:

- The user name of the creator of documents.
- The user name of the document owner.
- The user name of the person who is currently editing a document so that the document is locked.
- Permissions on folders for a user.
- ARIS document storage creates audit logs in a database. User names are stored in order to log document versions, changes on folder history.

These entries can be anonymized (page 9) for deleted users (page 6).

1.4 Process Governance + ARIS Process Board

Process Governance stores user names for different purposes, such as the delegation history and the execution of human tasks.

Process Governance creates audit logs in a database where user names are logged.

The data flow of an executable process step in Process Governance is described using a **Data flow diagram**. It has exactly one superior object from the control flow. This means that for objects that have multiple object occurrences in a business model, each of these object occurrences has its own data flow diagram.

This chapter describes the input and output parameters of services used in Process Governance and the different types of operators, constants and variables.

The **system** user and the **arisservice** user must always have the **Process Governance administrator** function privilege to execute services. The function privilege controls the tasks that users can perform. The **system** user is created automatically. By default, the system user has all function privileges. The user **arisservice** is created automatically. By default, this user is assigned the **Database administrator** and **Process Governance administrator** function privileges.

The Process Governance services can write user specific data to attributes. These attribute values can be anonymized with the help of customized reports in order to meet the requirements of the General Data Protection Regulation (GDPR (page 17)). Please contact your local Software AG sales organization (http://www.softwareag.com).

These entries can be anonymized (page 10) for deleted users (page 6).

1.5 ARIS Risk & Compliance Manager

In ARIS Risk & Compliance Manager user names are stored in object forms and lists and displayed as, for example, **Last editor**, **Performed by**. Deleted users can be anonymized (page 16).

1.6 Collaboration

The user name is stored Collaboration when a user creates a group, is coordinator of a group, follows a group, likes a post (), writes a comment. These entries can be anonymized for deleted users (page 6).

1.7 Pictures in ARIS Administration and Collaboration

If a user profile in ARIS Administration includes a picture, it is also displayed in Collaboration and vice versa. The data of both applications is automatically synchronized.

In ARIS Administration the picture of a user is deleted when the user is deleted in ARIS Administration. In Collaboration the picture of a user is deleted when the user was deleted in ARIS Administration and then anonymized (page 11).

1.8 ARIS Log Files

Many ARIS components save personal data, such as IP addresses, MAC addresses, and user names in log files, for example, **loadbalancer.log** or **agent.rest.operations.log**. ARIS handles log files in a cyclic way. Depending on the size or the age of a log file, new files are created and used. Older log files remain. If problems occur during operation, you can use log files to find and resolve errors.

In order to comply with the **G**eneral **D**ata **P**rotection **R**egulation (GDPR), you can collect log files using ACC (page 13) or the ACC interface (page 12), find personal data related to deleted users (page 6), and manually delete or anonymize log file entries in source files.

Warning

If you delete log files (page 14), Software AG might no longer be able to support you in order to resolve software problems.

1.9 PPM

Log files may contain private data of ARIS users, such as IP addresses, MAC addresses, or user names. In order to comply with the **G**eneral **D**ata **P**rotection **R**egulation (GDPR), please refer to the **PPM Operation Guide**. This guide explains how to handle personal data in PPM related log files.

2 How to delete and anonymize personal data

In order to comply to GDPR (page 17), after a defined period of time you must delete personal data of persons no longer employed. To do so, proceed as follows:

Delete users (page 6).

Anonymize personal data stored in User Management audit logs (page 7).

Anonymize personal user data remaining in ARIS databases (page 8).

Anonymize personal user data remaining in ARIS document storage (page 9).

Anonymize personal user data remaining in Process Governance (page 10).

Anonymize personal user data remaining in Collaboration (page 11).

Specify anonymization patterns in ARIS Risk & Compliance Manager (page 15).

Anonymize ARIS Risk & Compliance Manager users (page 16).

Anonymize log files entries (page 3).

2.1 Delete user

Delete users when they are no longer relevant.

Prerequisite

You have the **User administrator** function privilege.

Warning

Do not delete your system user. Having more than one system user can avoid problems. If your single system user was deleted accidentally, create a new one by using the superuser. The superuser cannot be deleted.

Procedure

1. Click  **User management**. The list of users is displayed.
2. Move the mouse pointer to the relevant user name. The buttons of the available functions are displayed.
3. Click **Delete**. The **Confirmation** dialog opens.
4. Click **OK**. The user data is deleted. It takes about 30 minutes until the deletion is written to the log files.
5. To comply with GDPR (page 17), delete the log files of ARIS Administration/User Management 30 minutes after deletion of the user data. You can find them in this path:

   <Your installation folder>\ARIS<version>\server\bin\work\work_umcadmin_<size>\base\logs
6. Delete the log files.

The user data and the log files are deleted.

To anonymize users according to GDPR (page 17), refer to the online help of the respective component.

Tip

To delete several users at the same time, enable the check boxes for the relevant users, and click **Delete**.

2.2 Anonymize User Management audit logs

You can anonymize deleted users in audit logs according to GDPR. Please use **y-tenantmgmt.bat** for Windows® operating systems and **y-tenantmgmt.sh** for Unix operating systems.

Please note that you must wait at least 30 minutes after the deletion of the user from User Management before you can start the anonymization process.

Prerequisites

- The user was deleted in ARIS Administration.
- ARIS must be running.
- ARIS Server installation

  Users need the function privileges **License administrator**, **User administrator**, **Technical configuration administrator**.
- Users need to login as **superuser** or they need either an **ARIS Architect** license or an **ARIS UML Designer** license. For LOCAL systems they need to login as system user **system**.

Procedure

1. Open a Command Prompt and navigate to:

   ARIS installation path>/server/bin/work/word_umcadmin_< your installation size, for example, s,m, or l> **/tools/bin** for Windows® operating systems

   and

   ARIS installation path>/cloudagent/bin/work/word_umcadmin_< your installation size, for example, s,m, or l> **/tools/bin** for Linux operating systems.
2. Enter this command to import all documents into ARIS document storage of each tenant you use, for example, **default**:

   y-tenantmgmt.bat -t <URL of the server> anonymize -u <user name> -p <password> -type user.

   If a user group is deleted, the **type** is **user group**.

   If the port used is other than the default ports **80** or **1080**, add the port to the URL.

The audit logs are anonymized.

2.3 Anonymize users (ARIS databases)

Users can only be deleted (page 6) in ARIS Administration.

Even if a user is deleted in the User Management of the ARIS Administration (page 6), in ARIS databases the user name stays visible in the **Creator** and the **Last modifier** model and object attributes, and in change list descriptions. This also applies to archived models and objects. You can anonymize user data according to GDPR (page 17).

Warning

Make sure to only anonymize deleted users. If you anonymize existing users, the user names are anonymized in all attributes, such as **Creator**, **Last modifier**, and the user names in change list descriptions.

Prerequisites

- **ARIS Server Administrator** is installed.
- You know the credentials of the superuser, or you have the Server administrator function privilege.
- The database must be locked for other users.

Procedure

1. Click **Start > Programs > ARIS > Administration > ARIS Server Administrator 10.0** if you accepted the program group suggested by the installation program. Under a Linux operating system, execute the **arisadm.sh** shell script instead. The command prompt opens and ARIS Server Administrator is launched in interactive mode.
2. Establish a connection to the server and tenant:

   syntax: **server <server name>:<port number> <tenant> <user name> <password>**

   Example: **server arissrv:1080 default system manager**
3. Enter **userwipeout <dbname>|all [<user>][,<user>]**.

User identifications of one or multiple users are deleted from one or all databases. The attributes **Last modifier**, **Creator**, and the user name in change list descriptions is set to **unknown**.

2.4 Anonymize ARIS document storage users

You can anonymize deleted users in ARIS document storage according to GDPR. Please use **y-admintool.bat** for Windows® operating systems and **y-admintool.sh** for Unix operating systems.

Prerequisites

- The user was deleted in ARIS Administration.
- ARIS must be running.

Procedure

1. Open a Command Prompt and navigate to:

   <ARIS installation path>/server/bin/work/work_apg_< your installation size, for example, s,m, or l> **/tools/bin** for Windows® operating systems

   and

   /home/ARIS/cloudagent/bin/work/work_apg_< your installation size, for example, s,m, or l> **/tools/bin** for Linux operating systems.
2. Enter this command to import all documents into ARIS document storage of each tenant you use, for example, **default**:

   y-admintool.bat -s <URL of ARIS document storage> -t <tenant name> anonymize -u <user name> -p <password>.

   If the port used is other than the default ports **80** or **1080**, add the port to the URL.

The users are anonymized.

Please note:

If you delete only one user from the user list or from user groups that have access to the folder and then anonymize the folder data, all actions related to the folder data are anonymized. This means that the anonymization does not affect the data of the deleted user only.

Before you delete a user, get the user ID of a specific user from the user details in the user management.

In this case, add the following parameter with **y-admintool.bat** or **y-admintool.sh**:

-ownerName <owner of the folder> -ownerType USER

2.5 Anonymize Process Governance users

You can anonymize deleted users of in Process Governance data, for example, in substitution logs or audit logs according to GDPR. All user names are replaced with **anonymous**. Please use **y-ageclitool.bat** for Windows® operating systems and **y-ageclitool.sh** for Unix operating systems.

Prerequisites

- The user was deleted in ARIS Administration.
- ARIS Server is running.

Procedure

1. Open a Command Prompt and navigate to:

   <ARIS installation path>/server/bin/work/work_apg_<s,m, or l> **/ tools / bin** for Windows® operating systems

   or:

   /home/ARIS/cloudagent/bin/work/work_apg_<s,m, or l> **/ tools / bin** for Linux operating systems.
2. Enter this command to import all documents into ARIS document storage of each tenant you use, for example, **default**:

   y-ageclitool.bat --apg <Process Governance endpoint> -ht <ID of the human task> -p <password of the executer> * -t <tenant name> -umc <user management endpoint> -u <user name of the executer>

The user name is replaced by the string **anonymous**.

2.6 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 is a command-line tool for administrating and configuring an ARIS installation. It communicates with ARIS Agents on all nodes.

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

   To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead. ACC is available if you have copied and installed the **aris10-acc-<number>** rpm file depending on the Linux operating system.

   Enter **help** or **help <command>** to get information about the usage of the commands.

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**.

2.7 Collect log files (ACC interface)

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. Open your browser and enter the URL:

   syntax: **http://<server name>:<port>/acc/ui**

   for example

   http://aris10srv.eur.co.umg:1080/acc/ui

   The infrastructure tenant's **login** dialog opens. The tenant cannot be changed. Having performed a standard installation, the **master** tenant is the infrastructure tenant by default.
2. Select the interface language.
3. Enter the **system** user's or the superuser's credentials.
4. Click **Log in**. The infrastructure tenant's **node** view is displayed. It gives an overview on the node's runnables.
5. If you want to collect all log files, click ⋮ **More >** **Download log files**.
6. If you want to only collect log files of a distinct runnable, move the mouse pointer to the related row and click **Download log file**.

A **ZIP** archive created to be opened or saved.

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 (http://www.softwareag.com/premiumsupport).

2.8 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 is a command-line tool for administrating and configuring an ARIS installation. It communicates with ARIS Agents on all nodes.

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

   To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead. ACC is available if you have copied and installed the **aris10-acc-<number>** rpm file depending on the Linux operating system.

   Enter **help** or **help <command>** to get information about the usage of the commands.

2. To collect log files, for example, related to the **abs_l** runnable enter:

   collect log files for abs_l

   To collect all log files enter:

   collect log files

   or

   collect logfiles

   You can use additional parameters. Enter **help** or **help <command>** to get information about the usage of the commands.

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 (http://www.softwareag.com/premiumsupport).

2.9 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 **G**eneral **D**ata **P**rotection **R**egulation (GDPR), you can collect log files using ACC (page 13) or the ACC interface (page 12), find personal data related to deleted users (page 6), and manually delete or anonymize log file entries in source files.

Warning

If you delete log files (page 14), 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 the related runnables to allow free file access to all files. If you do not stop the runnables, several files may be locked and cannot be deleted.

Procedure

1. Start ARIS Cloud Controller.
2. To delete log files, for example, related to the **abs_l** runnable enter:

   delete log files for abs_l

   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.

2.10 Specify anonymization patterns in ARIS Risk & Compliance Manager

Specify anonymization patterns according to GDPR (page 17) in order to anonymize deleted users in ARIS Risk & Compliance Manager. To distinguish the anonymized users from each other, a number is automatically added to the property value of the anonymized user ID/user name. This number is incremented by one for each additional anonymized user.

Prerequisites

You have the **System administrator** role.

Procedure

1. Start ARIS Risk & Compliance Manager.
2. Click **Administration > Configuration**.
3. Click **System configuration**. The configuration parameters are displayed.
4. To display the anonymization patterns, filter the system configuration by **GDPR**. The search result displays all **GDPR anonymization patterns** with their current values.
5. Click **Edit** in the row of the parameter you want to change. The **Specify parameter value** dialog opens.
6. Copy the current value to the **New value** box.
7. Make the relevant changes, for example, change the value that is to be displayed for the user ID.
8. Click **OK**.

The changes are immediately applied and stored in the database.

Click **Reset** in the row of the relevant parameter to reset the default value.

Now you can anonymize (page 16) users in ARIS Risk & Compliance Manager.

2.11 Anonymize ARIS Risk & Compliance Manager users

Anonymize users in ARIS Risk & Compliance Manager according to GDPR (page 17) after they were deleted in ARIS Administration and the data in ARIS Risk & Compliance Manager was synchronized.

Prerequisites

- You have the **System administrator** role.
- You have the **ARCM administrator** and the **User administrator** function privileges.

Procedure

1. Start ARIS Risk & Compliance Manager.
2. Click **Administration**.
3. Click **System management > Users**. The list is displayed.
4. Select the option **Yes** for the **Deactivated** filter and click **Apply filter**. The deactivated users are displayed.
5. Click the name of the user whose user data you want to anonymize. The form is displayed.
6. Click **Anonymize user**.
7. Click **OK** to confirm the dialog when you are prompted.

The user data is anonymized according to the patterns (page 15) specified.

If the anonymization patterns are changed at a later point but the same pattern must be applied to all anonymized users, repeat the anonymization for users who were anonymized before the pattern was changed.

Example

A dismissed employee is deleted from ARIS Administration. Then the user data in ARIS Risk & Compliance Manager is refreshed with user data based on ARIS Administration/User Management (Synchronize users with ARIS Administration/User Management). The user data is deactivated in ARIS Risk & Compliance Manager. However, there is still data containing the name of this user, such as objects the user edited. This user data must be anonymized.

3 Glossary

GDPR

The **G**eneral **D**ata **P**rotection **R**egulation (GDPR) protects the rights of individuals' personal data within the European Union. It also regulates the export of personal data outside the EU. GDPR is a regulation by the European Parliament, the Council of the European Union, and the European Commission.

PERSONAL DATA

Any information related to an identified or identifiable data subject, such as a natural person.

DATA PROTECTION OFFICER

Informs and advises the controller (page 17)/processor (page 17) of their obligations, monitors compliance, provides advice, and acts as the contact for the supervisory authority.

DATA PROTECTION REPRESENTATIVE

Represents the controller (page 17)/processor (page 17) with regard to their respective obligations under GDPR.

CONTROLLER

Determines the purpose and means of processing personal data. (Role according to article 4 of the GDPR.)

PROCESSOR

Processes personal data on behalf of the controller (page 17). (Role according to article 4 of the GDPR.)

4 Legal information

4.1 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 Software AG's consulting services, 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 only describe specific installations. It is not possible to document all settings and dependencies.

When you combine various technologies, please observe the manufacturers' instructions, particularly announcements concerning releases on their Internet pages. We cannot guarantee proper functioning and installation of approved third-party systems and do not support them. Always follow the instructions provided in the installation manuals of the relevant manufacturers. If you experience difficulties, please contact the relevant manufacturer.

If you need help installing third-party systems, contact your local Software AG sales organization. Please note that this type of manufacturer-specific or customer-specific customization is not covered by the standard Software AG software maintenance agreement and can be performed only on special request and agreement.

If a description refers to a specific ARIS product, the product is named. If this is not the case, names for ARIS products are used as follows:

Name	Includes
ARIS products	Refers to all products to which the license regulations of Software AG standard software apply.
ARIS Clients	Refers to all programs that access shared databases via ARIS Server, such as ARIS Architect or ARIS Designer.
ARIS Download clients	Refers to ARIS clients that can be accessed using a browser.

4.2 Disclaimer

ARIS products are intended and developed for use by persons. Automated processes, such as the generation of content and the import of objects/artifacts via interfaces, can lead to an outsized amount of data, and their execution may exceed processing capacities and physical limits. For example, processing capacities are exceeded if models and diagrams transcend the size of the

modeling area or an extremely high number of processing operations is started simultaneously. Physical limits may be exceeded if the memory available is not sufficient for the execution of operations or the storage of data.

Proper operation of ARIS products requires the availability of a reliable and fast network connection. Networks with insufficient response time will reduce system performance and may cause timeouts.

If ARIS products are used in a virtual environment, sufficient resources must be available there in order to avoid the risk of overbooking.

The system was tested using scenarios that included 100,000 groups (folders), 100,000 users, and 1,000,000 modeling artifacts. It supports a modeling area of 25 square meters.

If projects or repositories are larger than the maximum size allowed, a powerful functionality is available to break them down into smaller, more manageable parts.

Some restrictions may apply when working with process administration, ARIS Administration, ARIS document storage, and ARIS Process Board, and when generating executable processes. Process Governance has been tested and approved for 1000 parallel process instances. However, the number may vary depending on process complexity, for example, if custom reports are integrated.

ARIS document storage was tested with 40.000 document items. This includes documents, document versions or folders. We recommend monitoring the number and overall size of stored document items and archiving some document items if needed.