ARIS
TENANT MANAGEMENT

Version 10.0 - Service Release 3

December 2017

Document content not changed since release 10.0.2. It applies to version 10.0.3 without changes.

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.

Contents

1 Managing tenants

After the installation of ARIS Server two tenants are available.

The infrastructure **master** tenant manages administrative users and all other tenants.

The **default** tenant is available for operational use. If you need additional operational tenants to provide different sets of databases, users, configurations or ARIS methods you can easily create them. Additional tenants require a new set of ARIS licenses. Licenses must be unique in all tenants.

If you have installed an ARIS Server using an external database management system, all additionally created tenants are available as well. If you are going to create additional tenants for ARIS10.0 in order to migrate data from ARIS 9.8.7 or later, make sure to use identical names in both ARIS versions.

Administrators can manage tenants in different ways:

- Manage tenants using the Tenant Management tool (page 13)
- Tenant management using command line tools (page 22)
- Create tenants using ACC (page 3)
- Backup tenants using ACC (page 4)
- Restore tenants using ACC (page 7)
- Copy tenants using ACC (page 9)
- Delete tenants using ACC (page 11)

Please make sure to manage users and licenses for all tenants.

1.1 ARIS Cloud Controller (ACC)

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 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.

1.1.1 Create a tenant

After the installation of ARIS Connect 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 in order 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 (page 22) or Tenant Management (page 13).

Prerequisites

- ARIS Server installation
- Users need the **User administrator** function privileges:
- If you do not use the standard database system, make sure to create additional schemes in your Oracle or Microsoft SQL database management system and assign the tenants to these schemes (see ARIS Server Installation Guide).

Procedure

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

   create tenant <tenant name> username=<user name of a user holding the required privileges> password=<this user's password>.

   For tenant names please only use up to 30 lowercase ASCII characters and numbers. The name must begin with a character. Special characters and characters e. g. in Chinese, Cyrillic or Arabic cannot be used.

   e. g.:

   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, e. g.:

   create tenant test01 dba.user="system" dba.user.pwd="manager" dbinstance.id="db0000000000" default.tbl.space="ARISDATA" temp.tbl.space="TEMP" schema.name=aris_<tenant ID>" schema.pwd="*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 4).

1.1.2 Back up a tenant

You can back up a tenant data (page 6) using the ARIS Cloud Controller (ACC). Please note that no user can work on this tenant during the backup process.

Warning

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

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

Extensions, e.g., SSL certificates, SAP® Java Connector, and JDBC drivers, added using the **enhance** ACC command are not backed up.

Prerequisites

- ARIS Server installation
- Users need the function privileges:

  Analysis administrator

  ARCM administrator

  Collaboration administrator

  Database administrator

  Document administrator

  License administrator

  Process Governance administrator

  Server administrator

  Technical configuration administrator

  User administrator

  Dashboard administrator

  The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

Procedure

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

   backup tenant <tenant name> to <pathToBackUpFile> username=<user name of a user holding the required privileges> password=<this user's password>

   e. g:

   backup tenant default to "f:\\backupDefault.acb" username=y1234 password=managery1234.

   Notice the double backslashes. Alternatively, use a single forward slash.

The backup is started. The complete backup is written to one single zip file. You do not need to stop the Process Governance runnable to back up or restore Process Governance data. To avoid inconsistencies, you can't back up or restore Process Governance data while a process is still running. During a backup or restore, Process Governance is not accessible to avoid inconsistencies.

You can restore (page 7) this tenant using this zip 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 (page 22) or Tenant Management (page 13).

1.1.2.1 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. Extensions, e.g., SSL certificates, SAP® Java Connector, and JDBC drivers, added using the **enhance** ACC command are not backed up. In ARIS 10 all started runnables are automatically taken into account when executing tenant backup/restore commands.

Backup/restore	Required function privileges	Component (runnable)
Data from ARIS Administration, e.g., users, privileges,	User administrator Technical configuration administrator	ARIS Administration/User Management (umcadmin_<s, m, or l>)
Licenses User administration audit events are not part of the tenant backup.	License administrator	
System database Contains filters, templates, and font formats, but also ARIS Method and all evaluation scripts, macros and scheduled reports.	Server administrator	Modeling & Publishing (abs_<s, m, or l>)
ARIS databases	Database administrator	
Ad hoc analyses and queries	Analysis administrator	Analysis (octopus_<s, m, or l>)
ARIS document storage data Documents and access privileges	Document administrator Technical configuration administrator	ARIS document storage (adsadmin_<s, m, or l>)
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 & Compliance Manager data	ARCM administrator	ARIS Risk & Compliance Manager (arcm_<s, m, or l>)
Dashboards	Dashboard administrator	ARIS Aware (dashboarding_<s, m, or l>)

1.1.3 Restore a tenant

You can restore a tenant data (page 6) or copy the content of this tenant (page 9) to a different ARIS server. You need to have access to the relevant back-up zip 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.

Prerequisites

- You need access to the relevant back-up zip file.
- ARIS Server installation
- Users need the function privileges:

  Analysis administrator

  ARCM administrator

  Collaboration administrator

  Database administrator

  Document administrator

  License administrator

  Process Governance administrator

  Server administrator

  Technical configuration administrator

  User administrator

  Dashboard administrator

  The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

Procedure

1. Start ARIS Cloud Controller (ACC).
2. To restore the tenant, enter:

   restore tenant <tenant name> from <pathToBackUpFile> username=<user name of a user holding the required privileges> password=<this user's password>

   e. g:

   restore tenant default from "f:\\backupDefault.acb" username=y1234 password=managery1234.

   Notice the double backslashes. Alternatively, use a single forward slash.

   The tenant will be restored.

   Current data will be deleted and replaced. No user can work with this tenant during the restore process.
3. Make sure to change the standard user's passwords again.

The tenant is restored.

You can also create tenants using the ARIS Administration's command line tools (page 22) or Tenant Management (page 13).

1.1.4 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 zip 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, e.g., SSL certificates, SAP® Java Connector, and JDBC drivers, 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 function privileges:

  Analysis administrator

  ARCM administrator

  Collaboration administrator

  Database administrator

  Document administrator

  License administrator

  Process Governance administrator

  Server administrator

  Technical configuration administrator

  User administrator

  Dashboard administrator

  The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

Procedure

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

   stop <Process Governance instance>, e.g. stop apg_m
4. Enter:

   restore tenant <Tenant name> from <pathToBackUpFile> username=<user name of a user holding the required privileges> password=<this user's password>

   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:

   start <Process Governance instance>, e.g. 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 passwords of the **arisservice** user, the **guest** user, the **system** user and the **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 (page 22) or Tenant Management (page 13).

1.1.5 Delete a tenant

If you delete a tenant all information will be lost:

- 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

Prerequisites

- ARIS Server installation
- Users need the function privileges:

  Analysis administrator

  ARCM administrator

  Collaboration administrator

  Database administrator

  Document administrator

  License administrator

  Process Governance administrator

  Server administrator

  Technical configuration administrator

  User administrator

  Dashboard administrator

  The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

Procedure

1. Back up (page 4) the tenant in order to be able to restore (page 7) data again.
2. Start ARIS Cloud Controller (ACC).
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 the optional **force** keyword is used, the security question **Are you sure?** is overridden, i.e., the tenant and its data is deleted without further prompting the user.

The tenant has been deleted.

You can also manage tenants using the ARIS Administration's command line tools (page 22) or Tenant Management (page 13).

1.2 Tenant Management tool

The Tenant Management allows authorized users (page 19) to manage all tenants of the ARIS system's node (see Tenant Management online help).

If this node has been removed accidently, please make sure to add it again.

The Tenant Management user interface has been installed using the ARIS server setup program. It is run automatically with the user account of the user **superuser**. In order for other users to be able to log in (page 19), you have to configure the infrastructure tenant (page 14). This assigns users in the infrastructure tenant privileges for impersonation (page 20), along with additional function privileges.

Once all operational tenants are configured (page 15), impersonation enables users to assume the account of the system user **superuser** in order to perform administration tasks. After the ARIS server was updated, for all operational tenants make sure to specify **superuser** in the **Impersonation target users** field again.

If you want existing tenants that were not created using Tenant Management to be managed centrally, you have to adjust the configuration of these tenants (page 17).

1.2.1 Configure infrastructure tenant

In order for users to be able to log into Tenant Management, they must have been assigned **impersonation** privileges (page 20) by system users in this node's infrastructure tenant and also require additional function privileges. Impersonation enables users to use the account of the system user **superuser** to perform administration tasks. If this node has been accidentally removed, please make sure to add it again.

Prerequisite

You are a system user or have the **User administrator** and **Impersonation** function privileges.

Procedure

1. Click the link that was provided to you or that you have saved as a bookmark in your browser, e.g., **http://myServer:1080/umc**. The User Management login dialog opens.
2. Enter the name of the infrastructure tenant in the **Tenant** field, e.g., **master**.
3. Enter the user name **superuser** and the associated password.
4. Click **Log in**. The **User management** tab is displayed.
5. Click the user **superuser**.
6. Click **Privileges**. The list of function privileges is displayed.
7. Make sure that in addition to the assigned privileges at least the following function privileges are activated:
   - User administrator
   - Impersonation
   - Tenant administrator
   - Technical configuration administrator

The user **superuser** now has the required privileges in the infrastructure tenant.

If necessary, create users as substitutes and assign them the required function privileges in the same way.

For users to be able to use Tenant Management, you must configure all operational tenants (page 15).

1.2.2 Configure operational tenants

Impersonation enables users to use the account of the system user **superuser** to perform administration tasks.

To enable Tenant Management to establish connections to tenants, the user **superuser** must have all function privileges required for backup and restore in all operational tenants and must be defined as a target for impersonation.

Prerequisite

You are a system user or have the **User administrator** and **Impersonation** function privileges.

Procedure

1. Open ARIS Administration for an operational tenant, e.g., http://<server name>:<port>/#**default**/home).
2. Log in as a system user or a user with the **User administrator** and **Technical configuration administrator** function privileges.
3. Click **<user name> > Administration**. ARIS Administration opens.
4. Click the **Configuration** tab.
5. Click **User management**.
6. Select the **Users** entry in the drop-down list.
7. Click **General**.
8. Click **Edit**.
9. Click in the **Impersonation target users** field.
10. Enter the user name **superuser**.

    If the ARIS server was updated, make sure to reenter the user name for all operational tenants in the **Impersonation target users** field again.

11. Click **Save**. All users that have the **Impersonation** and **Tenant administrator** function privileges on the infrastructure tenant take on the identity of **superuser** and inherit all of the **superuser** privileges.
12. Click **User management**.
13. Select the user **superuser**. The details will be displayed.
14. Click **Privileges**. The list of function privileges is displayed.

15. Activate the function privileges required for backing up and restoring:
    - Analysis administrator
    - Collaboration administrator
    - Database administrator
    - Dashboard administrator
    - Document administrator
    - License administrator
    - Process Governance administrator
    - Server administrator
    - Technical configuration administrator
    - User administrator

    The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.
16. Log out of ARIS Administration.

    The user **superuser** has the privileges to manage data for the **default** tenant.
17. Enter the user **superuser** under **Impersonation target users** in all other operational tenants in your system in turn, and assign the required function privileges.

The user **superuser** has the privileges to manage all data for the tenants (page 21). All substitutes can log in using their user name and manage tenants on behalf of the system user **superuser**.

1.2.3 Configure existing tenants

To enable Tenant Management to establish connections to tenants that were not created using Tenant Management, you must adjust the configuration of these tenants.

Prerequisite

You are a system user or have the **User administrator** and **Technical configuration administrator** function privileges.

Procedure

1. Open ARIS Administration for an operational tenant, e.g., http://<server name>:<port>/#**default**/home).
2. Log in as a system user or a user with the **User administrator** and **Technical configuration administrator** function privileges.
3. Click **<user name> > Administration**. ARIS Administration opens.
4. Click the **Configuration** tab.
5. Click **User management**.
6. Select the **Users** entry in the drop-down list.
7. Click **General**.
8. Click **Edit**.
9. Click in the **Impersonation target users** field.
10. Enter the user name **superuser**.

    If the ARIS server was updated, make sure to reenter the user name for all operational tenants in the **Impersonation target users** field again.
11. Click **Save**. All users that have the **Impersonation** and **Tenant administrator** function privileges on the infrastructure tenant take on the identity of **superuser** and inherit all of the **superuser** privileges.
12. Select the **Security** entry in the drop-down list.
13. Click **Advanced settings**.
14. Click **Edit**.
15. Enable the **Generate user statistics** check box.
16. Click **Save**. The **Utilization** and **Licenses** columns can be displayed on the **Tenants** page.
17. Click **User management**.
18. Select the user **superuser**. The details will be displayed.
19. Click **Privileges**. The list of function privileges is displayed.

20. Activate the function privileges required for backing up and restoring:
    - Analysis administrator
    - Collaboration administrator
    - Database administrator
    - Dashboard administrator
    - Document administrator
    - License administrator
    - Process Governance administrator
    - Server administrator
    - Technical configuration administrator
    - User administrator

    The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.
21. Log out of ARIS Administration.

    The user **superuser** has the privileges to manage data for this tenant.
22. Configure all other tenants that were not created in Tenant Management in the same way.

The user **superuser** has the privileges to manage all data for the tenants (page 21). All substitutes can log in using their user name and manage tenants on behalf of the system user **superuser**.

1.2.4 Open Tenant Management

System users and users to whom the required privileges are assigned can log in to Tenant Management on the infrastructure tenant.

- They know the passwords for the system users **system** or **superuser**.
- They have login privileges.

Procedure

1. Click the link that was provided to you or that you have saved as a bookmark in your browser (syntax: <server name>:<port>/tm). The Tenant Management login dialog opens.

   The name of the infrastructure tenant is displayed. You cannot select any other.
2. Select the interface language. You cannot change the language once you have logged in.
3. Enter your user name and your password.

   Clicking **Forgot password** enables you to reset the password.

   If you reset the password for the user **system** or **superuser**, other users can no longer log in with these user names. Automated processes, e.g., automatic backups, can no longer be performed.
4. Click **Log in**.

You can manage all tenants in the system.

1.2.5 Which users can manage tenants?

The user **superuser** and users to which the required privileges are assigned by the user **superuser** can manage tenants.

If users with appropriate privileges start Tenant Management, they do this as the user **superuser**. This is facilitated by the **Impersonation** function privilege, which is assigned to relevant users on the infrastructure tenant (page 20).

1.2.6 What is impersonation?

Users manage tenants on behalf of the user **superuser**. This requires the **creation** of these users in the user management for the infrastructure tenant, e.g., master. To use impersonation, users require the **Impersonation** function privilege in the infrastructure tenant.

For Tenant Management, they also require the **User administrator**, **Tenant administrator**, and **Technical configuration administrator** function privileges.

In all other operational tenants, e.g., **default**, the user **superuser** must be defined as the target for impersonation. Impersonation enables users to back up tenants in which they do not exist as a user.

To back up and restore the data, the user **superuser** requires the following function privileges in all operational tenants:

- ARCM administrator
- Analysis administrator
- Collaboration administrator
- Dashboard administrator
- Document administrator
- Database administrator
- License administrator
- Process Governance administrator
- Server administrator
- Technical configuration administrator

1.2.7 What data is backed up and restored?

If you back up tenants manually or use a scheduled backup, the current state of the following data is saved in backup lists.

Tenant data is fully backed up only if the user executing the commands has sufficient privileges for all components in every tenant. Extensions, e.g., SSL certificates, SAP® Java Connector, and JDBC drivers, added using the **enhance** ACC command are not backed up. In ARIS 10 all started runnables are automatically taken into account when executing tenant backup/restore commands.

Backup/restore	Required function privileges	Component (runnable)
Data from ARIS Administration, e.g., users, privileges,	User administrator Technical configuration administrator	ARIS Administration/User Management (umcadmin_<s, m, or l>)
Licenses User administration audit events are not part of the tenant backup.	License administrator	
System database Contains filters, templates, and font formats, but also ARIS Method and all evaluation scripts, macros and scheduled reports.	Server administrator	Modeling & Publishing (abs_<s, m, or l>)
ARIS databases	Database administrator	
Ad hoc analyses and queries	Analysis administrator	Analysis (octopus_<s, m, or l>)
ARIS document storage data Documents and access privileges	Document administrator Technical configuration administrator	ARIS document storage (adsadmin_<s, m, or l>)
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 & Compliance Manager data	ARCM administrator	ARIS Risk & Compliance Manager (arcm_<s, m, or l>)
Dashboards	Dashboard administrator	ARIS Aware (dashboarding_<s, m, or l>)

You require the same function privileges to restore the data.

1.3 Command-line tool

The batch file **y-tenantmgmt.bat** can be used to manage tenants. Run it without argument to see the usage instructions.

Using some advanced ACC commands makes it possible to create a tenant, import a license and restore a database in one step. If you do not use the standard database system, please make sure to create additional schemes in your Oracle or Microsoft SQL database management system and you have assigned the tenants to these schemes.

You have to redirect the ports in case of a Linux operating system.

Prerequisites

- ARIS Server installation

  Users need the function privileges **License administrator**, **User administrator**, **Technical configuration administrator**.

- ARIS Design Server Installation

  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 (**Start > Run > cmd**).
2. Type **y-tenantmgmt.bat** without parameters to display the help.

   Type **y-tenantmgmt.bat -t <tenant name> <command> -u <user name> -p <password>** to enter a command. Parameters may differ.

General usage

Options	Description
-?, -h, --help	Show help, default: false
-s, --server	URL of the server, e.g. http://my_host_url:<port number other than default port 80 or 1080>

Commands	Description	Parameters
createTenant	Creates a new tenant.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory) For tenant names please only use up to 30 lowercase ASCII characters and numbers. The name must begin with a character. Special characters and characters e. g. in Chinese, Cyrillic or Arabic cannot be used. --arisservicePassword (-arisservicep) <PASSWORD> --superuserPassword (-superuserp) <PASSWORD> --systemPassword (-systemp) <PASSWORD>
listTenants	Lists all existing tenants.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory)
getTenant	Prints information about a tenant.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory)
deleteTenant	Deletes an existing tenant.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory)

Commands	Description	Parameters
createUser	Creates a new user.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory) --affectedUser (-au) <NEWUSERLOGIN> (mandatory) --affectedPassword (-ap) <NEWUSERPWD> --affectedFirstName (-af) <NEWUSERFIRST> --affectedLastName (-al) <NEWUSERLASTNAME> --affectedEmail (-ae) <NEWUSEREMAIL> --affectedDescription (-ad) <NEWUSERDESCR>
getUser	Prints information about a user.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory) --affectedUser (-au) <USERLOGIN> (mandatory)
updateUser	Updates an existing user.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory) --affectedUser (-au) <NEWUSERLOGIN> (mandatory) --affectedPassword (-ap) <NEWUSERPWD> --affectedFirstName (-af) <NEWUSERFIRST> --affectedLastName (-al) <NEWUSERLASTNAME> --affectedEmail (-ae) <NEWUSEREMAIL> --affectedDescription (-ad) <NEWUSERDESCR>
deleteUser	Deletes an existing user.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory) --affectedUser (-au) <USERLOGIN> (mandatory)
importConfig	Updates configuration of tenant.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory) --file (-f) <CONFIGFILE>
assignLicense	Assigns a license to a user.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory) --license (-l) <PRODUCTCODE> (mandatory) --affectedUser (-au) <USERNAME> (mandatory)

Commands	Description	Parameters
exportConfig	Exports configuration of tenant.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory) --file (-f) <CONFIGFILE>
importLicense	Imports license files for a tenant	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory) --file (-f) <LICENSEFILE>
unassignLicense	Removes a license from user.	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory) --license (-l) <PRODUCTCODE> (mandatory) --affectedUser (-au) <USERNAME> (mandatory)
listPrivilege	Lists the privileges of the user mentioned in the command	--user (-u) <USERNAME> (mandatory) --password (-p) <PASSWORD> (mandatory) --tenant (-t) <TENANTNAME> (mandatory)

After creating a tenant, you have to import the relevant license and create the users. You can do so from command line or via graphical user interface ARIS Administration.

It is recommended to change the password of the default user **system** immediately after the installation.

Examples

The following line creates a tenant with name **test**. Please pay attention to the order.

```
y-tenantmgmt.bat -s http://my_aris_host.com -t test createTenant -u system -p manager
```

The following line creates a new tenant with name **test01** and port 81 used and initial system user password **abc**. Please pay attention to the order.

```
y-tenantmgmt.bat -s http://my_aris_host.com:81 -t test01 createTenant -u system -p
manager -systemp abc
```

The following line gets information of the default tenant.

```
y-tenantmgmt.bat -s http://my_aris_host.com -t default getTenant -u system -p manager
```

The following line updates the configuration of default tenant.

```
y-tenantmgmt.bat -s http://my_aris_host.com -t default importConfig -f
sldapconfig.properties  -u superuser -p superuser
```

The following line assigns a license configuration to the user my_user.

y-tenantmgmt.bat -s http://my_aris_host.com-t default -assignLicense au my_user -l YCZUS -u system -p manager

1.4 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, e.g., if custom reports are integrated.

ARIS document storage was tested with 40.000 documents. We recommend monitoring the number and overall size of stored documents and if needed some documents should be archived.