

ARIS CONNECT
ADMINISTRATOR USER
MANUAL

VERSION 10.0 - SERVICE RELEASE 16
OCTOBER 2021

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 - 2021 Software AG, Darmstadt, Germany and/or Software AG USA Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <https://softwareag.com/licenses>.

Use of this software is subject to adherence to Software AG's licensing conditions and terms. These terms are part of the product documentation, located at <https://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <https://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Contents

1	ARIS Connect.....	1
2	Manage ARIS Connect.....	3
3	Open ARIS Administration	3
4	Manage licenses.....	4
4.1	License types and dependencies.....	4
4.2	Import and display license file	5
4.3	When is a license consumed?	6
4.4	Expired licenses	6
4.5	Enable or disable license monitoring.....	6
4.6	Delete licenses	7
4.7	Create and activate license rule.....	7
4.8	License rule types.....	8
4.9	Download and upload license rules	9
4.10	Generate License audit (password-protected) report	10
4.11	Generate License usage rule validation report	11
5	Manage users	12
5.1	Use case - Manage users	12
5.2	Create user	18
5.3	Make a user a system user.....	20
5.4	Copy a system user	21
5.5	Assign user groups to a user.....	23
5.6	Edit user	24
5.7	Log out user	25
5.8	Delete user	26
5.9	Delete all users/user groups	27
5.10	Default users.....	27
5.11	How can the password be changed?	29
5.12	Available licenses in ARIS Connect.....	30
5.13	Tenant-wide function privileges	31
5.14	Database-wide function privileges.....	33
5.15	Manage user groups.....	36
5.15.1	Create user group.....	36
5.15.2	Copy user group.....	37
5.15.3	Edit user group.....	38
5.15.4	Assign users to a user group	38
5.15.5	Delete user group	39
5.15.6	Delete all users/user groups.....	40
5.16	Assign privileges and profiles	40
5.16.1	Change a privilege for multiple users/user groups	40
5.16.2	Change multiple function, license, and database privileges for user/user group.....	41
5.16.3	Assign license pool to user group.....	44
5.16.4	Assign profiles to users/user groups.....	44
5.16.5	What function privileges can be assigned?	45
5.16.6	What license privileges can be assigned?.....	48

5.16.7	What is a configuration administrator?	49
5.17	Handle password	50
5.17.1	Change user password.....	50
5.17.2	Request new password.....	51
5.18	Apply LDAP.....	52
5.18.1	Import users/user groups from LDAP	52
5.18.2	Synchronize users/user groups with the LDAP system.....	53
5.19	Use SCIM	54
5.19.1	Generate bearer token	54
5.19.2	Copy bearer token to clipboard	55
5.19.3	Delete bearer token.....	56
5.20	Manage user data	57
5.20.1	Back up user management data	57
5.20.2	Restore user management data.....	58
5.20.3	Export user statistics.....	58
5.20.4	Generate report.....	59
5.20.5	Generate License audit (password-protected) report	60
5.20.6	Generate License usage rule validation report.....	61
5.20.7	Active sessions and history	62
5.20.8	ARIS Architect 'Administration' tab versus ARIS Administration	63
5.20.9	Which reports exist?	64
5.20.10	Delete and anonymize user accounts.....	64
5.20.11	What profiles include which content?	66
6	Configure jobs for ARIS document storage.....	67
7	Display charts for documents.....	68
8	Use ARIS document storage with WebDAV	69
9	Export statistics	70
10	Use metadata	71
10.1	Define custom metadata for documents	71
10.2	Delete custom metadata.....	72
10.3	Display document properties.....	72
10.4	Edit document properties	73
10.5	Generate a dashboard link.....	73
10.6	Edit document tags	74
10.7	Delete tags of a document	74
10.8	Change the document owner	75

11	Use folders	76
11.1	Create folder in ARIS document storage	76
11.2	Display folder details	76
11.3	Edit folder details	77
11.4	Move folders in ARIS document storage	77
11.5	Manage folder access for user groups	78
11.6	Manage folder access for users	79
11.7	Show assigned users or user groups	80
11.8	Exclude folder(s) from search	80
11.9	Delete folder in ARIS document storage	81
12	Good to know	82
12.1	What is ARIS document storage?	82
12.2	Access privileges for folders	82
12.3	Permanent documents	83
12.4	Temporary documents	83
12.5	Options for models or objects	84
12.6	External document management systems	84
12.7	Folder Dashboarding	84
12.8	Scheduled reports	86
12.9	Charts for documents	86
12.9.1	'Number of documents' chart	86
12.9.2	'Used space' chart	86
12.9.3	'Most viewed documents' chart	86
12.9.4	'Most changed documents' chart	87
12.9.5	'Largest documents' chart	87
12.9.6	'Latest documents' chart	87
12.9.7	'Document status overview' chart	87
12.9.8	'Outdated documents' chart	87
12.10	Delete and anonymize user accounts	88
13	Pages in ARIS document storage	89
13.1	ARIS document storage attribute types	89
13.2	Document details	90
13.3	Document history	92
13.4	Document relations	93
13.5	Document versions	94
13.6	Folder access privileges for user groups	95
13.7	Folder access privileges for users	96
13.8	Folder	97
13.9	Folder details	98
13.10	Folder history	99
13.11	Select document page	100
13.12	Select tags page	101
13.13	Upload document page	102
14	Administrate automated processes	103
14.1	Open process administration	103
14.2	What is 'Process administration' used for	103
14.2.1	What does 'Activities' provide?	104

14.2.2	What does 'Archive' and 'Archive history' provide?	105
14.2.3	What does 'Assignments' provide?	106
14.2.4	What does 'Console' provide?	106
14.2.5	What does 'Context' provide?	106
14.2.6	What does 'Details' provide?	106
14.2.7	What does 'Diagram' provide?.....	107
14.2.8	What does 'History' provide?.....	107
14.2.9	What does 'Human task' provide?	108
14.2.10	What does 'Instances' provide?	109
14.2.11	What does 'Variables' provide?	110
14.3	Tasks of the Process Governance administrator	110
14.4	Find process instances.....	111
14.5	Start governance process in process administration	111
14.6	Where can the executable process be started?.....	112
14.7	What is an executable process?	112
14.8	Context for executable processes.....	112
14.9	How many process instances can be started?	113
14.10	Export process administration content as a CSV file	113
14.11	Send reminder about executing human task	114
14.12	Suspend/resume execution of process instance	114
14.13	Terminate execution of process instance.....	115
14.14	Suspend/resume recurrence for executable process	116
14.15	Delete executable process	117
14.16	Suspend, resume, or terminate simulation runs.....	117
14.17	Use process instance archive	118
14.18	Prioritize and deprioritize process instances	120
14.19	How to handle large volume data	121
14.20	What is the escalation manager?	121
14.21	Find and correct problems in processes	121
14.21.1	List processes and display instance/version.....	122
14.21.2	Review input and output data of activity.....	123
14.21.3	Restart failed activities	124
14.21.4	Skip failed activities	125
14.21.5	Skip human tasks	126
14.21.6	Correct and restart failed process instances.....	127
14.22	Display information	128
14.22.1	Display information about executable processes.....	128
14.22.2	Display information about activities	129
14.22.3	Display human tasks of process instances	129
14.22.4	Display information about variables.....	130
14.22.5	Display and delegate executors of human tasks	130
14.22.6	Which status can activities have?	132
14.22.7	Which status can process instances have?.....	133
14.22.8	What statuses can tasks have?.....	134
14.23	Handle simulation	135
14.23.1	Display simulation information.....	135
14.23.2	Release simulated process.....	136
14.23.3	Delete simulation runs.....	136

15	Use charts	137
15.1	Display charts	137
15.2	What charts exist?	138
16	Configure ARIS Connect	139
16.1	Configure the user interface	139
16.1.1	Publish databases	140
16.1.2	Change sort order of published databases	141
16.1.3	Specify a default database	142
16.1.4	Allow model comparison	143
16.2	Configure user management	145
16.2.1	Import configuration	145
16.2.2	Export configuration	146
16.2.3	Configure user for impersonation	146
16.2.4	Impersonation	148
16.2.5	What is the default user group?	149
16.2.6	Customize infrastructure	150
16.2.7	Infrastructure properties	151
16.2.8	Kerberos	157
16.2.8.1	Customize Kerberos settings	157
16.2.8.2	Upload Kerberos configuration files	158
16.2.8.3	Kerberos properties	159
16.2.9	LDAP	164
16.2.9.1	Add LDAP server	164
16.2.9.2	Test connection to an LDAP server	165
16.2.9.3	Edit connection to an LDAP server	166
16.2.9.4	Upload LDAP truststore file	167
16.2.9.5	Customize LDAP settings	167
16.2.9.6	Customize ARIS for LDAP server operations	168
16.2.9.6.1	Configure secure communication	170
16.2.9.6.2	Allow login for LDAP users only	172
16.2.9.6.3	Configure single sign-on (LDAP)	173
16.2.9.6.3.1	Use Kerberos	174
16.2.9.6.3.2	Use SAML	177
16.2.9.7	Delete LDAP server	178
16.2.9.8	LDAP properties	179
16.2.9.9	Using multiple LDAP servers	200
16.2.10	User defined notifications	200
16.2.10.1	Customize user-defined notifications	200
16.2.10.2	Upload templates for notifications	201
16.2.10.3	Customize default HTML templates for notifications	202
16.2.10.4	Customize HTML templates for multiple locales	203
16.2.10.5	Properties for user-defined notifications	204
16.2.10.6	Variables for user-defined notifications	217
16.2.11	Customize password policy	218
16.2.12	Properties for password policies	219
16.2.13	SAML	229

16.2.13.1	Customize SAML settings	229
16.2.13.2	Upload keystore file.....	230
16.2.13.3	Upload truststore file	230
16.2.13.4	SAML properties.....	231
16.2.14	Customize security settings	243
16.2.15	Security properties.....	244
16.2.16	Customize SMTP settings.....	254
16.2.17	SMTP properties.....	255
16.2.18	Customize user settings	261
16.2.19	Properties for user settings	262
16.2.20	SCIM.....	270
16.2.20.1	Customize SCIM settings	270
16.2.20.2	Generate bearer token.....	271
16.2.20.3	Copy bearer token to clipboard	272
16.2.20.4	Delete bearer token.....	273
16.2.20.5	Specify SCIM client.....	273
16.2.20.6	SCIM properties.....	274
16.2.21	Customize Application switcher	281
16.2.22	Application switcher properties	282
16.2.23	What is ARIS Process Mining?.....	284
16.2.24	Customize OAuth 2.0 settings.....	284
16.2.25	OAuth 2.0 properties	285
16.3	Configure Document storage.....	288
16.3.1	Import configuration.....	288
16.3.2	Export configuration.....	289
16.3.3	Customize infrastructure settings	290
16.3.4	Infrastructure properties	291
16.3.5	Add third-party document management system - Basic Auth	299
16.3.6	Add a third-party document management system - OAuth	300
16.3.7	Test connection to a third-party document management system	301
16.3.8	Edit document management system.....	302
16.3.9	Delete third-party document management system	303
16.3.10	Properties for document management systems	304
16.3.11	Customize quota and restrictions	319
16.3.12	Properties for quota and restrictions.....	320
16.3.13	Configure full-text search	323
16.3.14	Properties for the full-text search.....	324
16.3.15	Configure WebDAV	330
16.3.16	WebDAV properties	331
16.4	Configure Process Governance.....	332
16.4.1	Import configuration.....	332
16.4.2	Export configuration.....	333
16.4.3	Set up sending notifications to Process Governance administrators.....	333
16.4.4	Customize notification settings	334
16.4.5	Enable/Disable HTML e-mail notifications	334
16.4.6	Customize HTML templates for e-mail notifications.....	335
16.4.7	What variables can you use?.....	336
16.4.8	Usable tags	337
16.4.9	List of allowed attributes inside each tag	339

16.4.10	Notification properties	340
16.4.11	Customize infrastructure settings	344
16.4.12	Infrastructure properties	345
16.4.13	Customize Publishing	353
16.4.14	Publishing properties.....	354
16.4.15	Customize Reporting	356
16.4.16	Reporting properties.....	357
16.4.17	Customize workflow policies	358
16.4.18	Properties for workflow policies.....	359
16.4.19	Customize pools.....	363
16.4.20	Properties for pools.....	364
16.5	Configure Collaboration	368
16.5.1	Customize Collaboration.....	368
16.5.2	Refresh list of published databases	368
16.5.3	Manually synchronize database.....	369
16.5.4	Properties for Collaboration.....	370
17	Manage server tasks	381
17.1	Display server tasks	381
17.2	Toggle auto-refresh	381
17.3	Cancel report	382
17.4	Good to know	383
17.4.1	What is the Server tasks area for?	383
17.4.2	How is the Running tasks list structured?	383
17.4.3	How is the Completed tasks list structured?	384
18	Make default dashboards available	385
18.1	Bulk Import using Command Line Tool	386
18.2	Copy documents using WebDAV	388
18.3	Import default dashboard content	389
18.4	Add a URL alias for dashboards.....	390
18.5	Check default data feeds for issues.....	391
18.6	Publish databases.....	392
18.7	Specify report parameters in ARIS Architect.....	393
18.8	Keep ARIS Aware dashboards up to date.....	395
18.9	Create user group.....	396
18.10	Using Matomo.....	397
18.10.1	Set up and configure Matomo	397
18.10.2	Add runnables	398
18.10.3	How to start ARIS Cloud Controller (ACC).....	401
18.10.4	Make an ARIS remote repository available.....	404
18.10.5	How to specify ARIS Aware Matomo reports	405
18.10.6	Report: Matomo - Database-specific portal usage.....	407
18.10.7	Report: Matomo - Global portal usage	408

19	Administrate Collaboration.....	409
19.1	Open Collaboration.....	409
19.2	Check activities flagged as inappropriate.....	410
19.3	Manage portal feeds.....	411
19.4	Synchronize access privileges.....	411
19.5	Manage announcements.....	412
19.6	Configure ARIS document storage user.....	412
19.7	Configure database user.....	413
19.8	Display dashboards.....	413
19.9	Clean up and export activities.....	415
19.10	Configure notifications.....	416
19.11	Customize e-mail notifications.....	417
19.12	Keyboard shortcuts for Collaboration.....	419
19.13	Privileges of coordinators and administrators.....	420
19.14	What is the synchronization user?.....	421
19.15	Delete and anonymize user accounts.....	421
19.16	Collaboration dashboards.....	422
19.17	Database access privileges for Collaboration.....	423
20	Manage SAP Solutions.....	424
20.1	Import portal configuration set providing SAP content.....	424
20.2	Select the View Providing SAP Content.....	425
20.3	Configure ARIS Online Guide.....	426
20.4	Publish databases in ARIS Connect (ARIS Online Guide).....	427
20.5	Make log files available.....	428
21	Configure Tenant Management.....	429
21.1	Configure infrastructure tenant.....	429
21.2	Configure user for impersonation.....	430
21.3	Configure operational tenants.....	431
21.4	Configure existing tenants.....	433
21.5	Open Tenant Management.....	433
21.6	Which users can manage tenants?.....	434
21.7	Impersonation.....	434
21.8	What data is backed up and restored?.....	435
22	Legal information.....	437
22.1	Documentation scope.....	437
22.2	Support.....	437
23	Index.....	i

1 ARIS Connect

This manual contains the descriptions of the online help, which refers to the administration of ARIS Connect. Users with **Administrator** function privileges can perform the described procedures.

ARIS Connect is an integrated environment in which you can create, display, and change processes, as well as discuss and improve them jointly with other ARIS Connect users. ARIS Connect provides role-based access to the content.

As a process expert, you receive access to the corresponding views and options for analyzing and improving processes.

In ARIS Connect projects participants can directly enter comments about modeled processes and discuss improvement potential with others. With dashboards KPIs can be visualized and controlled and relevant documents can be entered and distributed. The seamless integration with existing ARIS installations is ensured, which also allows users to cooperate concerning existing processes using integrated social media.

The functional scope of ARIS Connect depends on the license being used.

Here's what you can do:

- Manage licenses (page 4)
- Manage users (page 12)
- Manage user groups (page 36)
- Manage documents
- Administrate automated processes (page 103)
- Use charts (page 137)
- Set up user management (page 144)
- Set up ARIS document storage (page 287)
- Set up Process Governance (page 332)
- Set up Collaboration (page 368)
- Administrate Collaboration (page 409)
- Manage server tasks (page 381)
- Make default dashboards available (page 385)
- Manage SAP Solutions (page 424)
- Configure Tenant Management (page 429)

News on ARIS is available in ARIS Community.

(https://www.ariscommunity.com/system/files/files/ARIS_10_SR16_Features_Overview.pdf)

Note: You can watch videos for some procedures in the help. If your browser is unable to open the quick videos within the help, please use a different browser. The videos are also available in ARIS Community (<https://www.ariscommunity.com/help/quick-videos>).

Technical documents are available on:

- ARIS DVD 3 (...Documents\English\5 Customizing)
- Empower (<https://empower.softwareag.com/>) (login required)
- ARIS Download Center (<https://aris.softwareag.com/>)

2 Manage ARIS Connect

You can configure ARIS Connect so that it suits your needs.

Depending on which administrator privileges you have, you will have access to the areas described here where you can make the appropriate settings. For example, you can only see the user administration if you have the **User administrator** function privileges.



3 Open ARIS Administration

Centrally manage users, user groups, privileges, licenses, documents, and configurations for all ARIS products.

Prerequisite

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

Procedure

1. Click the link that was provided to you by e-mail or that you have saved as a bookmark in your browser. The **Login** dialog opens.
2. Enter your user name and your password.
3. Click **Log in**.
4. Click  **Application launcher** >  **Administration**.

ARIS Administration opens.

ARIS video tutorial

ARIS Architect 'Administration' tab versus ARIS Administration

(<https://www.ariscommunity.com/videos/aris-architect-administration-tab-versus-aris-administration-0>) (approx. 1 minute)

4 Manage licenses



Centrally manage licenses for all ARIS products to grant users the privileges required for the programs they use.

4.1 License types and dependencies

You can use only one license type for each product. Exceptions are the **Named user** and **Cross-client** license types.

LICENSE TYPES FOR CLIENT PRODUCTS

The license types for client products must be assigned manually to users or user groups. You can increase the number of licenses by installing additional licenses.

NAMED USER

Users assigned to this license type have guaranteed login as the license is registered in their name. The number of licenses that can be assigned is specified in the license file.

CONCURRENT USER

For this license type, the number of users who can log in at the same time is specified. The assigned users share the available licenses. If the number of users logged in is the same as the number of available licenses, no other users can log in. The user must wait until another user logs off. However, the administrator can end (page 24) the sessions of users.

Difference between 'Named user' and 'Concurrent user' license type

	Concurrent user	Named user
Assignment	Via user or user group	Via user or user group
License volume	Unlimited	Limited number
Guaranteed login	No	Yes
Term of guaranteed login	Current session	Unlimited

CROSS-CLIENT

This license type corresponds to a license of the **Named user** type. However, it can be imported and used for various tenants. It is intended for administrators who manage several tenants. The assigned users can log in with all tenants.

SERVER LICENSES

The license types for server products are activated automatically after the import.

DEPENDENCIES WITHIN PRIVILEGES

- There are certain license privileges that you cannot assign to a user in combination with others. For example, you cannot assign ARIS Architect and ARIS Designer to a user at the same time.
- You can only activate the subgroups of a license privilege if the superior license privilege is activated. If you remove a superior license privilege of a user, the user also automatically loses the assignment to the subgroups.



4.2 Import and display license file


Import a license file to give users the required privileges for the programs.

Prerequisite

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

Procedure

1. Click  **Licenses > Product**.
2. Click  **Import license file**. The corresponding dialog opens.
3. Select the relevant license file.
4. Click **Upload**.

The license file is transferred. It is shown how many licenses were imported, as well as which licenses could not be installed and why. To display information about licenses, such as the expiration date, number of licenses, click the relevant license, and select  **Open license file**. The license file is displayed as an XML file.

If license exhaustion notification is enabled in **Configuration (User management > User-defined notifications > Licenses > Notify about license exhaustion)**, license administrators receive a notification once the specified number of licenses is reached.

You can now assign users the required license privileges. If you need additional licenses later, simply import the new license file as described above.


4.3 When is a license consumed?

A license is consumed as soon as a user logs in and a session is created. Please note that a license is not only consumed when a user starts working, like creating models in ARIS Connect or administrating processes. If various licenses are assigned to a user, the license with the higher value is consumed first.

Example

User A is assigned to the licenses **ARIS Connect Viewer** and **ARIS Connect Designer** (both **Concurrent user** license type). After login, the **ARIS Connect Designer** license is consumed.

4.4 Expired licenses

Expired licenses are marked in the license overview: . Users or groups can no longer be assigned. Login is impossible with an expired license.

Before deleting licenses, back up user data, if required, in order to be able to reuse (page 58) them when new license are available. In the configuration, you can specify that administrators are notified before a license expires.




4.5 Enable or disable license monitoring

You can customize the license monitoring as required.

Prerequisite


You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Licenses > Monitoring > Configuration**.
2. Click  **Edit**.
3. Enable () or disable () license monitoring. License monitoring is disabled by default.
4. The license monitoring interval is indicated in minutes. By default, it is set to 5 minutes and should not be changed because this value guarantees an optimum outcome for the report evaluation (page 11).
5. Click  **Save**.

Your settings are saved. If you enabled license monitoring, you can now generate the License usage rule validation report (page 11).



4.6 Delete licenses

You can delete license files when they have expired. Before deleting licenses, back up user data, if required, in order to be able to reuse (page 58) them when new license are available. In the configuration, you can specify that administrators are notified before a license expires. Expired licenses are marked in the license overview: . Users or groups can no longer be assigned. Login is impossible with an expired license.

Prerequisite

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

Procedure

1. Click  **Licenses > Product**.
2. Click the relevant product or a subgroup.
3. Move the mouse pointer over the relevant license. The buttons of the available functions are displayed.
4. Click  **Delete license file**.

The license file is deleted.



4.7 Create and activate license rule

Create license rules for the **License usage rule validation** report. You can have multiple license rules, but only one can be activated.

Prerequisite

You have the **Technical configuration administrator** function privilege.



Procedure

1. Click  **Licenses > Monitoring > Rules**.
2. Click **Create**. The corresponding dialog opens.
3. Enter a name and select the rule type (page 8).
4. Click **Create**. The license rule is created.
5. In the row of the newly created license rule, click  **Edit license rule**. The fact sheet is displayed.
6. Under **License rule properties**, click **Edit**. The corresponding dialog opens.
7. If required, also enter the license rule name in other languages.


8. For **Aggregated weighting** rule types, enter a **Threshold**.
9. Click **Save**. The license rule properties are saved.
10. Create a license group for the license rule. To do so, click **Add** under **License groups**. The corresponding dialog opens.
11. Enter a license group name. If required, also enter the name in other languages.
12. For **Aggregated weighting** license rule types, click **Add**, select the relevant product codes, for example, **ARIS Connect Viewer(YCSCC)** and **ARIS Connect Designer(YCSDC)**, and enter a weighting for each.

For **Base & Peak** license rule types, click **Add**, select the relevant product codes, and enter a limit for each.

For **DBP** license rule types, enter a **Threshold** and select the relevant product codes.
13. Click **Save**.

The license group for the license rule is created.
14. Click  **Back**. The **Application management** page is displayed.
15. In the row of the newly created license rule, click  **Activate license rule**.

The license rule is created and activated. From now on, you can generate the License usage rule validation report (page 11).

To delete a license rule, click  **Delete** in the row of the relevant license rule.

4.8 License rule types

You can select the following license rule types when you create a license rule (page 7).

AGGREGATED WEIGHTING

A threshold is specified for the license rule and a weighting is assigned to each product contained in the license rule. The number of unique users who are consuming licenses from the license group is multiplied by the respective weighting of the license. If the calculated total value exceeds the threshold, the license usage exceeds the purchased license volume.

Example

The license group contains ARIS Connect Designer licenses (weighting = 10) and ARIS Connect Viewer licenses (weighting = 5). The specified threshold is 100. At a given point in time, nine users are logged in with ARIS Connect Designer licenses and two with ARIS Connect Viewer licenses. The calculated value of the consumed licenses is 100 (= 9 x 10 + 2 x 5) and therefore the license usage is not exceeded. As soon as an additional unique user logs in, the threshold is exceeded.

BASE & PEAK

A limit is specified for each product contained in the license rule. If the number of unique users who are consuming licenses from the license group exceeds the specified limit of the respective product, the license usage exceeds the purchased license volume.

Example

The license group contains ARIS Connect Designer licenses (limit = 10) and ARIS Connect Viewer licenses (limit = 5). At a given point in time, ten users are logged in with ARIS Connect Designer licenses and four with ARIS Connect Viewer licenses. Therefore, no limit is exceeded (base). As soon as an additional user logs in with ARIS Connect Designer license, the limit specified for this product is exceeded (peak).

DBP (DIGITAL BUSINESS PLATFORM)

The maximum number of products (threshold) and the products that can be concurrently used within a license group are specified (license bundle). Furthermore, a user should not use more than one license of a product concurrently. If the number of unique users who are consuming licenses from the license group exceeds the specified threshold, or if a user logs in with both products, the license usage exceeds the purchased license volume.

Example

The license bundle of the license group contains ARIS Connect Designer licenses and ARIS Connect Viewer licenses. The specified threshold is 10. At a given point in time, nine users are logged in with ARIS Connect Designer licenses and an additional user is logged in with ARIS Connect Viewer license. As soon as the user who is logged in with ARIS Connect Viewer license logs in with ARIS Connect Designer license, the threshold is exceeded.



4.9 Download and upload license rules

You can download and upload license rules as JSON file. The license rules are also included in the backup of user management data (page 57).

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Licenses > Monitoring > Rules**.
2. In the row of the license rule you want to download, click  **Download license** rule. The corresponding dialog opens.
3. Select **Save File** and click **Ok**.

The license rule file is saved as JSON file in the selected folder.

4. To upload a license rule file, click **Upload** above the list of license rules. The corresponding dialog opens.
5. Click **Select file**. The corresponding dialog opens.
6. Navigate to the JSON file you want to upload as a license rule.
7. Select the relevant file, then click **Open**.
8. Click **Upload**.


The license rule is displayed in the list of license rules.

Before you use it as the active license rule for the **License usage rule validation** report, check whether the license rule properties and the license groups are still valid. Example: If you uploaded a license rule from an older ARIS Connect version, check whether the product codes used for the license group exist in the system.




4.10 Generate License audit (password-protected) report

If your contract with Software AG contains a term under which you must regularly provide the usage data of the purchased licenses, generate the **License audit (password-protected)** report. This report is applicable to **Concurrent** and **Named user** licenses. For detailed information, contact your local Software AG sales organization (<https://www.softwareag.com/corporate/company/global/offices/default.html>).

Prerequisite

- You have the **User administrator**, **Configuration administrator**, and **License administrator** function privileges.
- **License monitoring** is enabled in  **Licenses > Monitoring > Configuration**.

Procedure



1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Generate report**. The corresponding dialog opens.
4. Select **License audit (password-protected)** report.
5. Click **Run**.

The report is output as a password-protected ZIP file containing an Excel file and a JSON file. Send this password-protected report to Software AG for evaluation.




4.11 Generate License usage rule validation report

Generate a report that lists the license usage based on the license rule. This report is applicable to **Concurrent** and **Named user** licenses.

Prerequisite

- You have the **User administrator**, **Configuration administrator**, and **License administrator** function privileges.
- License monitoring is activated (page 6) ( **Licenses > Monitoring > Configuration**).
- An active license rule is available (page 7) ( **Licenses > Monitoring > Rules**).

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Generate report**. The corresponding dialog opens.
4. Select **License usage rule validation** report.
5. Click **Run**.

The report is output as an Excel file.

5 Manage users



Users and privileges are managed centrally in ARIS Administration for all ARIS products. The role-dependent data access is controlled by privileges and filters that are assigned per database in ARIS Architect on the **Administration** tab.

5.1 Use case - Manage users



This use case provides a comprehensive description of all procedures that administrators must carry out for a tenant so that all authorized employees can work with ARIS Architect. We recommend that you use ARIS Administration to manage users, user groups, privileges, licenses, documents, configurations, and processes in ARIS Connect. This is what the use case is based on. Using User Management is advisable only for users of ARIS Risk & Compliance Manager, ARIS Publisher, PPM, and MashZone.


Scenario

After installation, the following system users exist: 'superuser' and 'system'. They are responsible for the user management of an activated tenant. The server was started, the password for the system user **superuser** has not been changed yet.

USER MANAGEMENT IN ARIS ADMINISTRATION



Procedure

1. Open ARIS Administration and log in as 'superuser'.
 - a. Click the link that was provided to you by e-mail or that you have saved as a bookmark in your browser. The **Login** dialog opens.
 - b. Enter your user name and your password.
 - c. Click **Log in**.
 - d. Click  **Application launcher** >  **Administration**.
ARIS Administration opens.
2. Change the passwords for the users 'superuser' and 'system'.
 - a. Change the passwords of the users **superuser** and **system** to prevent unauthorized access to the system. These users are created automatically after installation and have comprehensive function privileges and authorizations.
 - b. Click the user whose password you want to change.

- c. Click  **Edit**.
- d. Enable the **Change password** check box. The **Old password**, **New password**, and **Confirm password** fields are displayed.
- e. Enter a new password, and reenter it. If you want to use the webMethods integration, passwords must not contain a colon.
- f. Click **Save**.


The password is changed. The user receives a notification by e-mail.

3. Import the license purchased.

- a. Click  **Licenses > Product**.
- b. Click  **Import license file**. The corresponding dialog opens.
- c. Select the relevant license file.
- d. Click **Upload**.

The license file is transferred. It is shown how many licenses were imported, as well as which licenses could not be installed and why.

4. Create users.



- a. Click  **Add user**. The **Create user** form opens.
- b. Enter the user name, first and last name, e-mail address, if applicable, and password. If no password was specified for the user, a password is automatically generated for the first login and sent to the user. After the first login, the password must be changed. If a user that already exists in the LDAP system is created, the user name must match. The e-mail address is transferred automatically. For the other specifications you can enter any characters you wish because this information will automatically be transferred from the LDAP system after the user is created.

The user name does not necessarily have to correspond to a person's first or last name. To comply with the GDPR, a randomly selected character string is used, or an abbreviation of the first and/or last name.

- c. Click **Save**. The details view of the user is displayed.

The user is created. If no password was specified for the user, a password is automatically generated for the first login and sent to the user. After the first login, the password must be changed.



5. Alternatively, import LDAP users.

- a. Click  **Additional functions**.
- b. Click  **Start LDAP import**. The button is active only if an LDAP system is configured on the server.
- c. Select whether you want to import only users or user groups and associated users.

- d. Select if you want to use the default filter or create a custom one.
- e. Click **Preview** to check how many users or user groups are imported. The number is displayed, as well as up to 100 elements to be imported in alphabetical order.
- f. Click **Start import**.



The users or user groups and associated users are transferred from the LDAP system according to the selected options.

6. Create user groups.

- a. Click  **User management** and select **User groups**. The list of user groups opens.
- b. Click  **Add user group**.
- c. Enter the name of the user group and an optional description.
- d. Click **Save**.


The user group is created.

7. Alternatively, import LDAP user groups.

- a. Click  **Additional functions**.
- b. Click  **Start LDAP import**. The button is active only if an LDAP system is configured on the server.
- c. Select whether you want to import only users or user groups and associated users.
- d. Select if you want to use the default filter or create a custom one.
- e. Click **Preview** to check how many users or user groups are imported. The number is displayed, as well as up to 100 elements to be imported in alphabetical order.
- f. Click **Start import**.

The users or user groups and associated users are transferred from the LDAP system according to the selected options.



8. Assign a user group to the user.

- a. Click the user whose user group association you want to change.
- b. Click **Associated user groups**.
- c. Click  **Edit assignment**. The **Associate user groups** dialog opens.
- d. Enable the check boxes of the relevant items in the **Available user groups** box, and click ► **Add**. The user groups are transferred to the **Associated user groups** box.
- e. Click **OK**.

The user group is assigned to the user.

9. Assign function privileges to the user, if required.

- a. Click the user you wish to assign function privileges to. The user data is displayed.
- b. Click **Privileges**. The list of function privileges is displayed.

- c. Enable  the check boxes of the privileges whose assignment you want to add.
The user is assigned the selected privileges. This provides the user with privileges for functions (for example, the **Database administrator** function privilege).
10. Assign license privileges to the user.
 - a. Click the user you wish to assign license privileges to. The user data is displayed.
 - b. Click **Privileges**. The list of function privileges is displayed.
 - c. Click **License privileges**.
 - d. Enable  the check boxes of the privileges whose assignment you want to add.
The user is assigned the selected privileges. This provides the user with access to the ARIS products relevant to him.

Users can now log in with their assigned privileges.





For each ARIS database, you can grant access privileges to user groups or users.

Product-specific privileges are assigned in each ARIS product.

USER MANAGEMENT IN ARIS ARCHITECT




Procedure

These actions can also be carried out by users with the **Database administrator** and **User administrator** function privileges.






1. Start ARIS Architect.
2. Log in as **system** user and connect to the **default** tenant.
Please use the new password that you just changed in ARIS Administration. ARIS Architect starts.
3. Create databases. All users with the **Database administrator** function privilege can do so.
4. Click **ARIS >**  **Administration** or **ARIS >**  **Explorer**.
5. Click  **Navigation** in the bar panel if the **Navigation** bar is not activated yet.
6. In the Explorer tree, right-click your connection to the ARIS Server and select  **New >**  **Database**.
7. Enter a name. Do not use any special characters.
8. Enable the **Versionable** check box if you want the content of the new database to be versioned.
9. Click **OK**. The database is created and displayed in the **Navigation** bar, either as a  non-versionable or  versionable database.
All users and user groups are automatically transferred from ARIS Administration.
10. Assign access privileges.

11. Assign function privileges to users and user groups.
12. Assign filters to users and user groups.

The database is available to authorized users.

1. Assign access privileges for database groups. These actions can be carried out by all users with the **User administrator** function privilege.
2. Click **ARIS >  Explorer**.
3. Log in to the database.
4. Click  **Navigation** in the bar panel if the **Navigation** bar is not activated yet.
5. Right-click the group for which you want to edit the access privileges, and select  **Properties**.
6. Click **Access privileges (users)** or **Access privileges (user groups)** on the **Selection** tab.
7. Select the users/user groups for which you want to assign privileges.
8. Select the required access privileges. You can assign **Read (r)**, **Write (w)**, and **Delete (d)** access privileges. The **Version (v)** access privilege is available for versionable databases only. The selection is displayed in the **Privileges** column.
9. If you click the **Pass on privileges** button, the selected access privileges are applied to all subgroups. This also applies to all new subgroups created below this group in the future.
10. Click **OK**.

After the user logs in to the database again the changed access privileges will be in effect.

1. Assign database-specific function privileges to users and user groups.
2. In ARIS Architect, click **ARIS >  Administration**.
3. Click  **Navigation** in the bar panel if the **Navigation** bar is not activated yet.
4. Log in to the database.
5. In the **Navigation** bar, click  **Users** or  **User groups**.
6. In the table, right-click the user or user group, and select  **Properties**.
7. Click **Function privileges** on the **Selection** tab.
8. In the **Assign** column, click the relevant function privileges. You can assign only function privileges that are assigned to you, too.






You cannot change function privileges for system users.

If you selected **User** in the **Navigation** bar and are logged on as system user, you can enable the **System user** check box. This user receives all function and access privileges.

9. Click **OK**.

The function privileges are now assigned for this database.

For users to be able to view specific content of the database, you assign access privileges to them.

1. Assign filters to users and user groups.
2. In ARIS Architect, click **ARIS** >  **Administration**.
3. Click  **Navigation** in the bar panel if the **Navigation** bar is not activated yet.
4. Log in to the database.
5. In the **Navigation** bar, click  **Users** or  **User groups**.
6. In the table, right-click the user or user group, and select  **Properties**.
7. Click **Method filter** on the **Selection** tab.
8. In the **Assign** column, enable the checkboxes of the relevant filters.
9. Click **OK**.

The selected filters are assigned. Users can now log in using these filters.

You can select a default filter for each database. This filter is automatically assigned when you create users and user groups.

All users with the corresponding privileges can work with ARIS Architect.

For new databases, these privileges must be assigned by authorized users.

ARIS video tutorial

ARIS Architect 'Administration' tab versus ARIS Administration

(<https://www.ariscommunity.com/videos/aris-architect-administration-tab-versus-aris-administration-0>) (approx. 1 minute)

5.2 Create user

Create a user for authorized employees. The default users (page 27) **system**, **superuser**, **arisservice**, and **guest** are created automatically. You can create additional system users (page 20).

Prerequisite



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

Warning


If this user is also modeled in an organizational chart, all differing data and assignments are overwritten when the executable process is subsequently generated or the organizational chart is updated. This does not apply to LDAP users.







To prevent this, enable the attribute **Consider user group association from user management**.



Procedure

1. Click  **User management**. The list of users is displayed.
2. Click  **Add user**. The **Create user** form opens.
3. Enter the user name, first and last name, e-mail address, if applicable, and password. If no password was specified for the user, a password is automatically generated for the first login and sent to the user. After the first login, the password must be changed. If a user that already exists in the LDAP system is created, the user name must match. The e-mail address is transferred automatically. For the other specifications you can enter any characters you wish because this information will automatically be transferred from the LDAP system after the user is created.

The user name does not necessarily have to correspond to a person's first or last name. To comply with the GDPR, a randomly selected character string is used, or an abbreviation of the first and/or last name.

4. Click **Save**. The details view of the user is displayed. If no password was specified for the user, a password is automatically generated for the first login and sent to the user. After the first login, the password must be changed.
5. Assign a user group to the user, if required.
6. Click **Associated user groups**.
7. Click  **Edit assignment**. The **Associate user groups** dialog opens.

8. Enable the check boxes of the relevant items in the box of the available items, then click **► Add**. The items are transferred to the box of the associated items. To remove items from the associated items box, enable the check boxes of the relevant items in this box, and click **◀ Remove**. To associate all available items, click **► Add all**, and click **◀ Remove all** to remove all items.
9. Click  **Save**.
10. Click **Privileges**. The list of function privileges is displayed. A distinction is made between privileges assigned directly and those assigned via a user group.
11. Enable () the check boxes of the privileges whose assignment you want to add. In order to make a user a system user, enable all function privileges.
12. Click **License privileges**. A distinction is made between privileges assigned directly and those assigned via a user group.
13. Enable () the check boxes of the privileges whose assignment you want to add.
14. To manage access privileges for the entire database, click **Database privileges**. To manage access privileges on a database group level, use  **Configuration > Databases** instead.
15. Enable () the check boxes of the privileges whose assignment you want to add.
16. Click  **Edit**. The **Edit database privileges** dialog opens.
17. Select the relevant privilege from the list.
18. Click **OK**.

The user is created with the corresponding user group and privilege assignments. The user cannot be created if a mandatory field was not filled out or a user name was entered that is already in use by another user in the system. LDAP users are indicated by a different symbol () than the other users (.

Additional information about the user is displayed under Attributes.

To transfer a user's group and privilege assignments to a new user, go to the overview of users and click **Copy user** in the row of the relevant user. Enable the check box of assignments to be transferred and add the remaining data, such as user name, first and last name, etc. of the new user.



5.3 Make a user a system user

Create additional system (page 27) users. Having more than one system user can avoid problems, if, for example, your single system user has forgotten his password.

Prerequisite

You have the **User administrator** function privilege. If all users including the system users are deleted, use the superuser. The superuser cannot be deleted.

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click the relevant user. The user data is displayed.
3. Click  **Edit**.
4. Click **Privileges**. The list of function privileges is displayed.
5. Enable all check boxes.

Now, the user is a system user. The **system** user has all function privileges. This user can log in to process administration, ARIS Administration, User Management, and My tasks. In ARIS Architect and ARIS Designer, this user has all access privileges for all database groups of all databases.

If your only system user was deleted accidentally, create a new one by using the superuser.






MAKE A USER A SYSTEM USER FOR A SPECIFIC DATABASE

System users have all function and access privileges in a database. To be on the safe side, create additional system users besides the system user **system**.

Prerequisite

- You have the **ARIS Enterprise Administration** license privilege.
- You have the **Database administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**.
2. Click  **Configuration**.
3. Click **Databases**.
4. Select the database and click  **Properties** >  **Function privileges**.
5. Click **Users** and use the filter to navigate to the related user that you want to make a system user for this database.
6. Enable the **System user** check box.

The user receives all function and access privileges for this database. This affects the privileges in ARIS only. The function privileges of a user in ARIS Administration are not affected.

To reject system user privileges, clear the respective check boxes. If the **Database administrator** function privilege was assigned to a user in ARIS Administration, this user has full access to all databases of the tenant. For such users, you cannot disable the **System user** check box. System users can only revoke privileges from users that are system users in single databases.

5.4 Copy a system user

Copy an existing system (page 27) user. Having more than one system user can avoid problems, if, for example, your single system user has forgotten his password.

Prerequisite



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

Warning

If this user is also modeled in an organizational chart, all differing data and assignments are overwritten when the executable process is subsequently generated or the organizational chart is updated. This does not apply to LDAP users.

To prevent this, enable the attribute **Consider user group association from user management**.

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click the relevant user. The user data is displayed.
3. Click  **Copy**. The **Copy user** form opens.
4. Enable **Transfer function privileges**.
5. Enable **Transfer user group associations** and/or **Transfer license privileges**, if required.
6. Enter the user name, first and last name, e-mail address, if applicable, and password. If no password was specified for the user, a password is automatically generated for the first login and sent to the user. After the first login, the password must be changed. If a user that already exists in the LDAP system is created, the user name must match. The e-mail address is transferred automatically. For the other specifications you can enter any characters you wish because this information will automatically be transferred from the LDAP system after the user is created.

The user name does not necessarily have to correspond to a person's first or last name. To comply with the GDPR, a randomly selected character string is used, or an abbreviation of the first and/or last name.

7. Click  **Save**.

An additional system user is created. The **system** user has all function privileges. This user can log in to process administration, ARIS Administration, User Management, and My tasks. In ARIS Architect and ARIS Designer, this user has all access privileges for all database groups of all databases. If no password was specified for the user, a password is automatically generated for the first login and sent to the user. After the first login, the password must be changed.



5.5 Assign user groups to a user

You can change the assignment of user groups for a user. User groups define the tasks or functions that a person performs in a company. A certain set of function, license, and database privileges, as well as profiles, is assigned to different user groups. If a user group is assigned to a user, the user has all privileges and profiles assigned to that user group. A user can belong to several different user groups at the same time. Function and license privileges can be assigned through the group or directly to the user. The type of assignment is displayed in **Users > <user name> > Privileges**.

Prerequisite

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

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click the user whose user group association you want to change.
3. Click **Associated user groups**.
4. Click  **Edit assignment**. The **Associate user groups** dialog opens.
5. Enable the check boxes of the relevant user groups in the **Available user groups** box, and click ► **Add**. The user groups are transferred to the **Associated user groups** box. To remove user groups from the **Associated user groups** box, enable the check boxes of the relevant user groups in this box, and click ◀ **Remove**. To associate all available items, click ► **Add all**, and click ◀◀ **Remove all** to remove all items.
6. Click **OK**.

The user groups assigned to the user have been changed.

If required, product-specific groups must additionally be created and assigned in each ARIS product.




5.6 Edit user

Edit user accounts. You cannot change the user name. If you are using an LDAP system, you cannot change the password either.

Prerequisite

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

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click the user whose data you want to change. The user data is displayed.
3. To change or delete a user's picture, click  **Change picture**. If a different picture is uploaded in ARIS Administration or in Collaboration, it is automatically transferred to the other application.
4. Click  **Edit**.
5. Change the relevant information, such as name, e-mail address, etc.
6. To change a password, enable **Change password**. The **Old password**, **New password**, and **Confirm password** fields are displayed.
7. Click **Save**.
8. Enter a new password, and reenter it. If you want to use the webMethods integration, passwords must not contain a colon.
9. Change the user group assignment (page 23), if necessary.
10. If required, change the profile or the function, license, and database privileges for the user (page 41).

The user's data is changed. After you have changed the password, the user is informed per e-mail about the new password.

5.7 Log out user



You can end the sessions of users. This can be necessary, for example, if all licenses of the **Concurrent user** license type (page 4) are used up because users have forgotten to log out. It can also be useful to end sessions if the assignment of function or license privileges was changed, as these privileges only take effect after users have logged in again.

Prerequisite

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

LOG OUT SINGLE USER


Procedure

1. Click  **User management**. The list of users is displayed.
2. Click the user you wish to log out. The user data (details) is displayed.
3. Click **Active sessions**.
4. Click  **Log out user**.
5. Click **OK**.

The user is logged out and can log back in again.

LOG OUT MULTIPLE USERS USING A SPECIFIC LICENSE

Procedure

1. Click **Privileges**, and select **License privileges**.
2. Click the license privilege for which you want to log out users.
3. Click **Active sessions**.
4. Enable the check boxes of the users you want to log out.
5. Click  **Log out user**.
6. Click **OK**.

The users are logged out.

To obtain an overview of all users currently logged in, export (page 58) a user statistics.

5.8 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 (page 27). 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 (page 27). The superuser cannot be deleted.

If you delete the default users system, arisservice, and guest, the **Generate, if not available** option (**ARIS Administration > Configuration > User management > Users >**) is automatically disabled and the users are no longer generated at startup with the last saved password until you manually enable the option again. The superuser can recreate the other default users (**system, arisservice, guest**) if they were 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, 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 delete several users at the same time, enable the check boxes for the relevant users, and click  **Delete**. Make sure not to enable any check boxes of default users (system, arisservice, guest), as they cannot be deleted by bulk deletion. They can only be deleted individually like described above. To anonymize users according to GDPR, refer to the online help of the respective component (page 64).

5.9 Delete all users/user groups




If you want to set up user management from scratch, you should delete all users and user groups. This is recommended before you change to or deactivate LDAP, for example.

The superuser cannot be deleted. The other default users (page 27) **system**, **arisservice**, and **guest** can only be deleted individually (page 25). They are not deleted if you include them in bulk deletion ( **Remove all** or  **Delete**, with multiple users selected at a time).

Prerequisite

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

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Remove all**. The **Confirmation** dialog opens.
4. Click **OK**.

All users and user groups are deleted except for the default users.

5.10 Default users



Warning

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 (page 27) (**arisservice** user, **guest** user, **system** user, **superuser** user) on all operational tenants, as well as on the infrastructure tenant (master).

'SYSTEM' USER

The **system** user is created automatically. By default, the system user has all function privileges. This user can log in to process administration, ARIS Administration, User Management, and My tasks. In ARIS Architect and ARIS Designer, this user has all access privileges for all database groups of all databases. This user only uses up a license if a license privilege is activated for this user. The default password is **manager**. You should change the default password to prevent unauthorized access. You can change all user data except for the user name.



Having more than one system user can avoid problems, if, for example, your single system user has forgotten his password. You can create (page 20) additional system users or copy

(page 21) the existing system user. If your only system user was deleted accidentally, create a new one by using the superuser. The user can only be deleted individually (page 25). Enable the **Generate, if not available** option ( **Application launcher** >  **Administration** > **Configuration** > **User management** > **Users** >) so that the user is automatically generated again at startup with the last saved password.



'SUPERUSER'

The user **superuser** is created automatically. By default, this user is assigned the **User management, License management, and Configuration administrator** function privileges. This user can also enable this function privilege for other users. Users of the **superuser** type do not use up a license. They manage the system administration, but cannot use ARIS products due to license restrictions. The default password is **superuser**. You should change the default password to prevent unauthorized access. The password of the superuser is very important, as it is the only user who cannot be deleted. You can change all user data except for the user name. The superuser can recreate the other default users (**system, arisservice, guest**) if they were deleted.

'ARISSERVICE' USER

The user **arisservice** is created automatically. By default, this user is assigned the **Database administrator and Process Governance administrator** function privileges. This user only uses up a license if a license privilege is activated for this user. The default password is **arisservice**. You should change the default password to prevent unauthorized access. You can change all user data except for the user name. The user can only be deleted individually (page 25). Enable the **Generate, if not available** option ( **Application launcher** >  **Administration** > **Configuration** > **User management** > **Users** >) so that the user is automatically generated again at startup with the last saved password.

'GUEST' USER

The user **guest** is created automatically. By default, no function or license privileges are assigned to this user. This user serves technical purposes only. It is not for use by end users. Logging in to ARIS Connect or other Software AG products with this user is not allowed. Further information is available in the Software AG license terms (<http://softwareag.com/licenses>). The user can only be deleted individually (page 25). Enable the **Generate, if not available** option ( **Application launcher** >  **Administration** > **Configuration** > **User management** > **Users** >) so that the user is automatically generated again at startup with the last saved password.

5.11 How can the password be changed?

There are several possibilities for changing a user's password. Passwords of LDAP users cannot be changed.

PASSWORD IS CHANGED BY THE ADMINISTRATOR

A user with the **User management** function privilege can change the passwords of other users.

CHANGE PASSWORD MANUALLY

A password can be changed (page 50) manually in the user management (**Change password**).

GENERATE PASSWORD

Alternatively, a password can be generated (page 50) automatically in the user management (**Generate password**).

PASSWORD IS CHANGED BY THE USER

The user has two possibilities for changing his password in the login dialog.

CHANGE PASSWORD

If a user's password has expired, he will be asked to change it in the login dialog (**Change password**). The user will receive an e-mail containing the new password.

RESET PASSWORD

If the user has forgotten his password, he can request a new one (**Reset password**). The rest of the procedure depends upon whether a one-stage or two-stage password change is enabled (**Administration > Configuration > User management**). For the one-stage change the user immediately receives an e-mail with the new password. For a two-stage change the user first receives an e-mail asking him to confirm the resetting of his password within a specific period of time. The user receives a new password after he has confirmed.

5.12 Available licenses in ARIS Connect

For working with ARIS Connect, the **Designer** and **Viewer** licenses are available.

DESIGNER

- The **ARIS Connect Designer** license gives users access to the entire repository. They can access models, documents, and dashboards and feeds. In the **Models & Object** area, for example, users can create, edit, and delete models in databases.
- The **ARIS Connect Designer** license can be extended with the **ARIS Aware** license. The **ARIS Aware** license allows users to see and configure dashboards for which they have view rights. The users can see the dashboards, for example, in the Dashboards fact sheet.

VIEWER

- The **ARIS Connect Viewer** license enables users to view models in databases. This means that these users use databases for review and information purposes.
- The **ARIS Connect Viewer** license can be extended with the **ARIS Aware** license. The **ARIS Aware** license allows users to see configured dashboards for which they have view rights. The users can see the dashboards, for example, in the Dashboards fact sheet.
- The **Contribution** license is an additional license to users using an **ARIS Connect Viewer** license. If you have both the **ARIS Connect Viewer** and **Contribution** license privilege, you can change the values of specific model types and objects, create new or reuse existing items, as well as delete items in the **Content** view.

5.13 Tenant-wide function privileges

Function privileges provide users with specific functions and control their privileges. Additionally, the user must be assigned to a license privilege. You can assign (page 41) the following function privileges to users or user groups. Tenant-wide function privileges are assigned in ARIS Administration. Depending on your license, the offered function privileges may vary.

ARCM ADMINISTRATOR

Manage ARIS Risk & Compliance Manager system settings and run data exports/imports.

ARCM SYNCHRONIZATION ADMINISTRATOR

Synchronize databases, models, or groups from ARIS Connect or ARIS to ARIS Risk & Compliance Manager.

ARIS CONNECT ADMINISTRATOR

Specify which version of which database is to be published in the portal, and manage the corporate design.

ANALYSIS ADMINISTRATOR

Back up, restore, and manage the analysis database of a tenant. Import and export queries and ad hoc analyses.

ANALYSIS PUBLISHER

Publish and delete ad hoc analyses and queries for other users. Back up ad hoc analyses and queries.

COLLABORATION ADMINISTRATOR

Manage private groups, flagged posts, announcements, and e-mail templates.

COMPONENT ADMINISTRATOR

Add, start, stop, and remove components on the ARIS Cloud Controller server.

CONFIGURATION ADMINISTRATOR

Configure ARIS Server, export and import a tenant's configuration files, for example, ARIS filters, templates, and XML structures.

CONFIRMATION ADMINISTRATOR

Manage confirmation processes in ARIS Connect.

DASHBOARD ADMINISTRATOR

Create and manage visual content in ARIS Connect, for example, dashboards.

DATABASE ADMINISTRATOR

Manage tenant databases. System user in all databases.

DOCUMENT ADMINISTRATOR

Manage documents, document versions, folders, and access privileges in ARIS document storage.

IMPERSONATION

Manage data in other tenants using impersonated users and their privileges.

LICENSE ADMINISTRATOR

Use ARIS Administration/User Management to import, export, or delete licenses.

PORTAL ADMINISTRATOR

Manage the portal's corporate design.

PPM USER

Use PPM.

PROCESS GOVERNANCE ADMINISTRATOR

Manage Process Governance processes.

PUBLISHER ADMINISTRATOR

Generate, update, and delete ARIS Publisher exports.

PUBLISHING ADMINISTRATOR

Specify which version of which database is to be published in the portal.

SCRIPT ADMINISTRATOR

Manage report scripts and macros of a tenant.

SERVER ADMINISTRATOR

Query and terminate sessions on ARIS Server. Back up and update the system database, and display database statistics and all databases.

SERVICE ADMINISTRATOR

Register external systems and services (for example, external database systems, mail servers, or proxy servers) on the ARIS Cloud Controller server.

TECHNICAL CONFIGURATION ADMINISTRATOR

Configure systems, such as LDAP or SMTP, use ARIS Administration/User Management to import or export configuration files, and manage documents.

TENANT ADMINISTRATOR

Create, back up, restore, and delete tenants on the ARIS Cloud Controller server.

UML VIEWER

View UML content in ARIS Connect.

User administrator

Manage users, user groups, and privileges in ARIS Administration/User Management.

5.14 Database-wide function privileges

You can assign function privileges to provide users and user groups with specific functionality and thus control their authorizations across a database. Function privileges for databases are assigned in ARIS Architect on the properties pages of users or user groups.

Attribute formatting

Users with this function privilege can format attributes.

Change Management

Users with this function privilege can:

- modify proposals
- propose and modify measures
- specify end dates for measures
- set priorities
- define persons responsible

Database backup

Users with this function privilege can back up the database.

Database export

Users with this function privilege can:

- transfer database content to other databases (merge)
- export and import database content.

Database management

Users with this function privilege can:

- edit database properties
- edit database attributes
- create, modify, and delete languages

Database reorganization

Users with this function privilege can reorganize the database.

Font format management

Users with this function privilege can create, change, or delete font formats in the database on the **Administration** tab.

Lock permanently

Users with this function privilege can lock group content, objects, and models during Release Cycle Management. Permanently locked database items are displayed, but they can only be edited by the user who locked them. This user and, in ARIS Architect, system users can remove the lock.

Method changes

Users with this function privilege can change the color or line weight of objects in models by changing the **Fill color**, **Line color**, **Line style**, and **Weight** boxes on the **Format > Representation > Object appearance** page.

As a result, only the appearance of this object occurrence differs from the default appearance defined in ARIS Method.

To change ARIS Method you need the **Configuration administrator** function privilege in ARIS Administration.

Prefix management

Users with the **Prefix management** function privilege can manage database prefixes and change this attribute for all database items for which they have the **Write** access privilege.

Prefixes of a database are managed on the **Administration** tab on the **Identifier** properties page. By assigning a particular prefix to a user, you can identify the users who have created database items.

Report automation

Users with the **Report automation** function privilege can run reports as scheduled reports. The group **Scheduled reports** is displayed in the Explorer tree.

Show user management

Displays the database items **Users** and **User groups** on the **Administration** tab. Users with this function privilege cannot edit users/user groups.

User management

Displays the database items **Users** and **User groups** on the **Administration** tab.

Users with this function privilege can edit user groups and users who are not system users.

- Assign method filters
- Assign function privileges
- Assign access privileges
- Specify default method filter

Users can only assign privileges which they have themselves.

5.15 Manage user groups

User groups define the tasks or functions that a person performs in a company. A certain set of function, license, and database privileges, as well as profiles, is assigned to different user groups. If a user group is assigned to a user, the user has all privileges and profiles assigned to that user group. A user can belong to several different user groups at the same time.



5.15.1 Create user group

Create a new user group. User groups define the tasks or functions that a person performs in a company. A certain set of function, license, and database privileges, as well as profiles, is assigned to different user groups. If a user group is assigned to a user, the user has all privileges and profiles assigned to that user group. A user can belong to several different user groups at the same time.

Prerequisite

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

Procedure

1. Click  **User management** and select **User groups**. The list of user groups opens.
2. Click  **Add user group**.
3. Enter the name of the user group and an optional description. If a user group that already exists in the LDAP system is created, the user group names must match. This is the only way to assign an existing ARIS user group with the LDAP user group.
4. Click **Save**.

The user group is created. Now, you can assign users to the user group (page 38).

If required, product-specific groups must additionally be created and assigned in each ARIS product.

Tip

To transfer user and privilege assignments of a group to a new group, go to the overview of groups and click **Copy group** in the row of the relevant group. Enable the check box of assignments to be transferred and add the remaining data, such as group name, etc. of the new group.



5.15.2 Copy user group

You can copy user groups.

Prerequisite

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

Procedure

1. Click  **User management** and select **User groups**. The list of user groups opens.
2. Move the mouse pointer over the user group you want to copy. The buttons of the available functions are displayed.
3. Click  **Copy user group**.
4. Click **Transfer user associations** to assign the users of the group copied to the new group.
5. Click **Transfer privilege assignments** to assign the function privileges of the group copied to the new group. License privileges are transferred only with the **Concurrent user** license type. For the other license types, the license privileges must be assigned (page 40) in a separate step.
6. Enter the name of the user group.
7. Click **Save**.

The user group is created based on the group copied. If applicable, assign the group the required license privileges.

If required, product-specific groups must additionally be created and assigned in each ARIS product.



5.15.3 Edit user group

You can change user group data. If required, product-specific groups must additionally be created and assigned in each ARIS product.

Prerequisite

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

Procedure

1. Click  **User management** and select **User groups**. The list of user groups opens.
2. Click the user group whose data you want to change.
3. Click  **Edit**.
4. Change the description, if necessary.
5. Click **Save**.
6. Change the user assignment (page 38), if necessary.
7. Change the function privileges for the user group, if necessary.

The user group data is changed.




5.15.4 Assign users to a user group

You can change the assignment of users for a user group. Function and license privileges can be assigned through the group or directly to the user. The type of assignment is displayed in **Users > <user name> > Privileges**.

Prerequisite

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

Procedure

1. Click  **User management** and select **User groups**. The list of user groups opens.
2. Click the user group whose user association you want to change.
3. Click **Associated users**.
4. Click  **Edit assignment**. The **Associate users** dialog opens.
5. Add all users you want to assign to the group. Use the  **Filter** to limit the list of users, based on specific search criteria.

Enable the check boxes of the relevant items in the box of the available items, then click ► **Add**. The items are transferred to the box of the associated items. To remove items from the associated items box, enable the check boxes of the relevant items in this box, and click ◀ **Remove**. To associate all available items, click ► **Add all**, and click ◀ **Remove all** to remove all items.

6. Click **OK**.

The users associated to the user group have been changed.

If required, product-specific groups must additionally be created and assigned in each ARIS product.



5.15.5 Delete user group

You can delete user groups that are no longer relevant.


Prerequisite

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

Procedure



1. Click  **User management** and select **User groups**. The list of user groups opens.
2. Move the mouse pointer over the relevant user group name. The buttons of the available functions are displayed.
3. Click  **Delete**. The **Confirmation** dialog opens.
4. Click **OK**.

The user group is deleted.

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

5.15.6 Delete all users/user groups




If you want to set up user management from scratch, you should delete all users and user groups. This is recommended before you change to or deactivate LDAP, for example.

The superuser cannot be deleted. The other default users (page 27) **system**, **arisservice**, and **guest** can only be deleted individually (page 25). They are not deleted if you include them in bulk deletion ( **Remove all** or  **Delete**, with multiple users selected at a time).

Prerequisite

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

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Remove all**. The **Confirmation** dialog opens.
4. Click **OK**.

All users and user groups are deleted except for the default users.

5.16 Assign privileges and profiles







5.16.1 Change a privilege for multiple users/user groups

Assign a function or a license privilege for multiple users or user groups.

Prerequisite

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

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click **Privileges**. The list of function privileges is displayed.
3. Click the function privilege you want to assign. The current assignment is displayed.
4. Click  **Edit assignment**. The **Associate users/user groups** dialog opens.
5. Enable the check boxes of the relevant items in the box of the available items, then click  **Add**. The items are transferred to the box of the associated items. To remove users/user groups from the **Associated users/user groups** box, enable the check boxes of the relevant users/user groups in this box, and click  **Remove**. To associate all available items, click  **Add all**, and click  **Remove all** to remove all items.

6. Click **OK**.
7. Click **License privileges**. The list of license privileges is displayed.
8. Repeat steps 3 - 5 to assign a license privilege to multiple users or user groups.

The user/user group is assigned the corresponding privileges. If users are assigned a privilege directly and via associated user groups, this is detected automatically so that the user only uses one license.

5.16.2 Change multiple function, license, and database privileges for user/user group

Assign the relevant function, license, and database privileges to allow usage of specific programs and functions. Product-specific privileges are assigned in each ARIS product.

There are certain license privileges that you cannot assign to a user in combination with others. For example, you cannot assign ARIS Architect and ARIS Designer to a user at the same time.


You can only activate the subgroups of a license privilege if the superior license privilege is activated. If you remove a superior license privilege of a user, the user also automatically loses the assignment to the subgroups.

Prerequisite

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



CHANGE FUNCTION, LICENSE, AND DATABASE PRIVILEGES FOR INDIVIDUAL USERS

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click the user whose privileges you want to change.
3. Click **Privileges**. The list of function privileges is displayed. A distinction is made between privileges assigned directly and those assigned via a user group.
4. Enable ()/disable () the check boxes of the privileges whose assignment you want to add/remove.

In order to make a user a system user, enable all function privileges.




5. Click **License privileges**. A distinction is made between privileges assigned directly and those assigned via a user group.
6. Enable ()/disable () the check boxes of the privileges whose assignment you want to add/remove.

7. To manage access privileges for the entire database, click **Database privileges**. To manage access privileges on a database group level, use  **Configuration > Databases** instead.
8. Enable ()/disable () the check boxes of the privileges whose assignment you want to add/remove. No database privileges are assigned yet.
9. Click  **Edit**. The **Edit database privileges** dialog opens.
10. Select the relevant privilege from the list.
11. Click **OK**.

The user is assigned the selected privileges. The assignment of these privileges is displayed as **Granted** in the overview of function and license privileges for a user.

CHANGE FUNCTION PRIVILEGES FOR ALL MEMBERS OF A USER GROUP

Procedure

1. Click  **User management** and select **User groups**. The list of user groups opens.
2. Click the user group whose privileges you want to change.
3. Click **Privileges**. The list of function privileges is displayed.
4. Enable ()/disable () the check boxes of the privileges whose assignment you want to add/remove.
5. Click **License privileges**.
6. Enable () the check boxes of the privileges whose assignment you want to add.
7. To manage access privileges for the entire database, click **Database privileges**. To manage access privileges on a database group level, use  **Configuration > Databases** instead.
8. Enable ()/disable () the check boxes of the privileges whose assignment you want to add/remove. No database privileges are assigned yet.
9. Click  **Edit**. The **Edit database privileges** dialog opens.
10. Select the relevant privilege from the list.
11. Click **OK**.

All members of the user group are assigned the selected privileges. The assignment of these privileges is displayed as **Via user group** in the overview of function and license privileges for a user.

Product-specific privileges are assigned in each ARIS product.

The following special features apply for process automation:

If the **Process Governance administrator** function privilege has been assigned to the user in the model but not in user management, the user is also assigned the **Process Governance administrator** function privilege in user management the next time the executable process is generated. If the user has the **Process Governance administrator** function privilege from user management but not from the model, the **Process Governance administrator** function privilege is removed from the user in user management the next time the executable process is generated.



5.16.3 Assign license pool to user group

Assign a number of licenses (license pool) exclusively to a user group.

Prerequisite

- You have the **User administrator** function privilege.
- License pools at user group level is enabled in ARIS Administration configuration (**Security > Advanced settings**).
- The used license type (page 4) is **Concurrent user**.

Procedure

1. Click  **User management** and select **User groups**. The list of user groups opens.
2. Click the user group whose license limit you want to change.
3. Click **Privileges > License privileges**.
4. Move the mouse pointer over the relevant license. The buttons of the available functions are displayed.
5. Click  **Change licenses**. The corresponding dialog opens.
6. Enable the **Granted** check box.
7. Enter the number of licenses you want to assign in the **Assigned licenses** box.
8. Click **Save**.

The licenses are assigned to the user group.

5.16.4 Assign profiles to users/user groups


Assign the relevant profile (page 65) to enable a profile-based view of the portal. Depending on the profile, the information and functionality that users have access to varies. Example: For users to which the **Viewer** profile is assigned, the **Steps** fact sheet is displayed when a model is selected. They are unable to view the **Tasks** fact sheet and the **Contribute** function as they do not have an active role. Profiles are applied in addition to the function (page 45) and license (page 48) privileges.

Prerequisite

- Assignment of profiles is enabled in ARIS Administration configuration.
- You have the **User administrator** function privilege.

ASSIGN PROFILES TO INDIVIDUAL USERS

Procedure


1. Click  **User management**. The list of users is displayed.
2. Click the user you want to assign a profile to. The user data is displayed.
3. Click **Privileges > Profiles**. The list of profiles is displayed. A distinction is made between profiles assigned directly and those assigned via a user group.
4. Enable/disable the check boxes of the profiles whose assignment you want to add/remove.

The user is assigned the selected profiles.

If more than one profile is assigned, the user can switch between these profiles via **<user name> > Profiles > <profile_xy>**. Only one profile can be active at a time.

ASSIGN PROFILES TO ALL MEMBERS OF A USER GROUP

Procedure

1. Click  **User management** and select **User groups**. The list of user groups opens.
2. Click the user group you want to assign a profile to. The user data is displayed.
3. Click **Privileges > Profiles**. The list of profiles is displayed.
4. Enable/disable the check boxes of the profiles whose assignment you want to add/remove.

All members of the user group are assigned the selected profiles. The assignment of these profiles is displayed in the overview of profiles for a user as **Via user group**.

If more than one profile is assigned, the user can switch between these profiles via **<user name> > Profiles > <profile_xy>**. Only one profile can be active at a time.

5.16.5 What function privileges can be assigned?

Function privileges provide users with specific functions and control their privileges.

Additionally, the user must be assigned to a license privilege. You can assign (page 41) the following function privileges to users or user groups. Additional privileges can be assigned in each ARIS product at the database level.

ARCM ADMINISTRATOR

Manage ARIS Risk & Compliance Manager system settings and run data exports/imports.

ARCM SYNCHRONIZATION ADMINISTRATOR

Synchronize databases, models, or groups from ARIS Connect or ARIS to ARIS Risk & Compliance Manager.

ARIS CONNECT ADMINISTRATOR

Specify which version of which database is to be published in the portal, and manage the corporate design.

ANALYSIS ADMINISTRATOR

Back up, restore, and manage the analysis database of a tenant. Import and export queries and ad hoc analyses.

ANALYSIS PUBLISHER

Publish and delete ad hoc analyses and queries for other users. Back up ad hoc analyses and queries.

COLLABORATION ADMINISTRATOR

Manage private groups, flagged posts, announcements, and e-mail templates.

COMPONENT ADMINISTRATOR

Add, start, stop, and remove components on the ARIS Cloud Controller server.

CONFIGURATION ADMINISTRATOR

Configure ARIS Server, export and import a tenant's configuration files, for example, ARIS filters, templates, and XML structures.

CONFIRMATION ADMINISTRATOR

Manage confirmation processes in ARIS Connect.

DASHBOARD ADMINISTRATOR

Create and manage visual content in ARIS Connect, for example, dashboards.

DATABASE ADMINISTRATOR

Manage tenant databases. System user in all databases.

DOCUMENT ADMINISTRATOR

Manage documents, document versions, folders, and access privileges in ARIS document storage.

IMPERSONATION

Manage data in other tenants using impersonated users and their privileges.

LICENSE ADMINISTRATOR

Use ARIS Administration/User Management to import, export, or delete licenses.

PORTAL ADMINISTRATOR

Manage the portal's corporate design.

PPM USER

Use PPM.

PROCESS GOVERNANCE ADMINISTRATOR

Manage Process Governance processes.

PUBLISHER ADMINISTRATOR

Generate, update, and delete ARIS Publisher exports.

PUBLISHING ADMINISTRATOR

Specify which version of which database is to be published in the portal.

SCRIPT ADMINISTRATOR

Manage report scripts and macros of a tenant.

SERVER ADMINISTRATOR

Query and terminate sessions on ARIS Server. Back up and update the system database, and display database statistics and all databases.

SERVICE ADMINISTRATOR

Register external systems and services (for example, external database systems, mail servers, or proxy servers) on the ARIS Cloud Controller server.

TECHNICAL CONFIGURATION ADMINISTRATOR

Configure systems, such as LDAP or SMTP, use ARIS Administration/User Management to import or export configuration files, and manage documents.

TENANT ADMINISTRATOR

Create, back up, restore, and delete tenants on the ARIS Cloud Controller server.

UML VIEWER

View UML content in ARIS Connect.

USER ADMINISTRATOR





Manage users, user groups, and privileges in ARIS Administration/User Management.

ARIS video tutorial

ARIS Architect 'Administration' tab versus ARIS Administration

(<https://www.ariscommunity.com/videos/aris-architect-administration-tab-versus-aris-administration-0>) (approx. 1 minute)

5.16.6 What license privileges can be assigned?

License privileges provide users with specific products and components. You can assign (page 41) the license privileges to users or user groups ( **Application launcher** >  **Administration** > **User management** > **Users** > <user name> > **Privileges** > **License privileges** or  **Application launcher** >  **Administration** > **User management** > **User groups** > **Privileges** > **License privileges**). Move the mouse pointer over a license privileges name to display the description. Additional privileges can be assigned in each ARIS product at the database level.

5.16.7 What is a configuration administrator?

Configuration administrators are authorized to adapt the configuration settings of a tenant. Therefore, they require the **Configuration administrator** function privilege (page 41). Configuration administrators can manage content only if they have the required function privileges related to the content.

Configuration administrators perform the following tasks depending on their additional function privileges:

- Configure user management (page 144) (**User administrator** function privilege required)
- Configure Document storage (page 287) (**Document administrator** function privilege required)
- Configure Process Governance (page 332) (**Process Governance administrator** function privilege required)
- Configure Collaboration (page 368) (**Collaboration administrator** function privilege required)

For advanced configuration, you need the **ARIS Enterprise Administration** license privilege (page 41). The **ARIS Enterprise Administration** license privilege additionally allows configuration administrators to do the following:

- Configure model types, object types and object symbols, connection types, attribute types and attribute symbols, and attribute type groups.
- Manage filters
- Manage configuration languages
- Manage font formats used in the Conventions section
- Manage model templates
- Manage content type sets
- Manage databases (**Database administrator** function privilege required)
- Manage evaluation scrips and macros.

5.17 Handle password

Assign a new password to a user or generate it automatically. You can request a new password if you have forgotten your current password.

5.17.1 Change user password



Assign a new password to a user or generate it automatically. Passwords of LDAP users cannot be changed.

Prerequisite

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

CHANGE PASSWORD MANUALLY



Procedure

1. Click  **User management**. The list of users is displayed.
2. Click the user whose password you want to change. The user data is displayed.
3. Click  **Edit**.
4. Enable the **Change password** check box. The **Old password**, **New password**, and **Confirm password** fields are displayed.
5. Enter a new password, and reenter it. If you want to use the webMethods integration, passwords must not contain a colon.
6. Click **Save**.

The password is changed. The user receives a notification by e-mail.

GENERATE PASSWORD

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click the user whose password you want to change. The user data is displayed.
3. Click  **Generate password**. The button is only displayed for users who are not LDAP users.

The password is changed. The user receives a notification by e-mail.

5.17.2 Request new password

You can request a new password if you have forgotten your current password. If an LDAP system is used for user management, please contact your LDAP administrator to request a new password.

Procedure

1. Click **Reset password** in the **Login** dialog. The corresponding dialog opens.
2. Enter your user name.
3. Click **Reset password**.

Depending on your configuration, you will either receive an e-mail with a new password immediately or you must first confirm your password change using a link.

5.18 Apply LDAP

You can import users from the LDAP system and you can synchronize user and user group data with the data stored in the LDAP system.




5.18.1 Import users/user groups from LDAP

You can import users from the LDAP system.

Prerequisite



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

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Start LDAP import**. The button is active only if an LDAP system is configured on the server.
4. Select whether you want to import only users or user groups and associated users.
5. Select if you want to use the default filter or create a custom one.
6. Click **Preview** to check how many users or user groups are imported. The number is displayed, as well as up to 100 elements to be imported in alphabetical order.
7. Click **Start import**.

The users or user groups and associated users are transferred from the LDAP system according to the selected options.



5.18.2 Synchronize users/user groups with the LDAP system

You can synchronize user and user group data with the data stored in the LDAP system. LDAP users are indicated by a different symbol () than the other users (.

Prerequisite

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

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click the user or user group you wish to synchronize.
3. Click  **Synchronize with LDAP**. The button is active only if an LDAP system is configured on the server.

Data is transferred from the LDAP system for the selected item.

5.19 Use SCIM

ARIS supports SCIM with SAML 2.0.

5.19.1 Generate bearer token





If you suspect that your bearer token is no longer safe, you can generate a new bearer token and hand it over to your SCIM administrator.

We recommend that you use your own local user who has the **Technical configuration administrator** function privilege and the **User administrator** function privilege. This user can generate a bearer token and forward it together with the SCIM end point URL (page 274) to the SCIM administrator.

Prerequisite

- You have the **User administrator** function privilege.
- SCIM is enabled and correctly configured in **ARIS Administration > Configuration > User management > SCIM**.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **User management**. The list of users is displayed.
3. Click your user. The bearer token is always user-specific. In principle one bearer token is sufficient system-wide.
4. Click **SCIM bearer token**.
5. Click  **Generate bearer token**. The dialog opens.
6. Click **OK** to confirm.

The new bearer token is generated.

Click **Copy** to copy the bearer token to the clipboard to hand it over to your SCIM administrator so that it can be imported.




5.19.2 Copy bearer token to clipboard

You can copy the bearer token to the clipboard to hand it over to your SCIM administrator so that he can import it.

Prerequisite

- You have the **User administrator** function privilege.
- SCIM is enabled and correctly configured in **ARIS Administration > Configuration > User management > SCIM**.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **User management**. The list of users is displayed.
3. Click your user. The bearer token is always user-specific. In principle one bearer token is sufficient system-wide.
4. Click **Copy** to copy the bearer token to the clipboard.

You can hand over the bearer token to your SCIM administrator so that he can import it.




5.19.3 Delete bearer token

You can delete a bearer token.

Prerequisite

- You have the **User administrator** function privilege.
- SCIM is enabled and correctly configured in **ARIS Administration > Configuration > User management > SCIM**.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **User management**. The list of users is displayed.
3. Click your user. The bearer token is always user-specific. In principle one bearer token is sufficient system-wide.
4. Click **SCIM bearer token**.
5. Click **Delete**.

The bearer token is deleted.

5.20 Manage user data

You can backup and restore management data, export user statistics and generate reports (page 64) about users, user groups, privileges, licenses, assignments, etc.


5.20.1 Back up user management data

You can create a backup file based on the data in user management. Optionally, you can include the user statistics.




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 have the **User administrator** function privilege.
- 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 (page 244) (see ARIS help: ARIS Administration >  Configuration > User management > Security > Advanced settings). By default, this property is disabled.

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Back up data**. The **Back up user management data** dialog opens.
4. Enter a password and confirm it. The password is required for restoring this file.
5. Optionally, you can include the user's photos in the data backup.
6. Click **Start**.

The user management data is saved in JSON format in a ZIP file. The file is separated into several areas to enable even large data volumes to be saved easily: users, user groups, user settings, licenses, license rules, pictures, privileges, configuration, and charts. Backups from an ARIS installation version 9.7 and older can be restored. Backups from the current ARIS installation cannot be restored in older versions.




5.20.2 Restore user management data

You can restore previously backed up user management data in Administration. Deactivate LDAP before restoring the data to speed up the process. Backups from an ARIS installation version 9.7 and older can be restored. Backups from the current ARIS installation cannot be restored in older versions.

Prerequisite

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

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Restore data**. The corresponding dialog opens.
4. Select the backup file.
5. Enter the password to open the file.
6. Click **Start**.

The user management data is restored.




5.20.3 Export user statistics

Export statistics about users. Optionally, you can export usage patterns, assignments, changes to data and database items made by the user, the information used most often or the information used last, etc.

Prerequisites

- You have the **User administrator** function privilege.
- **Generate user statistics (com.aris.umc.audit.enabled)** is enabled in the configuration (page 244) (**User management > Security > Advanced settings**). If **License monitoring (User management > License monitoring > General)** is enabled, **Generate user statistics** is automatically enabled.

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Export user statistics**. The corresponding dialog opens.

4. Select the information that the report should output (event type). Ensure that the maximum number of entries included do not exceed 500.000.
5. Select the output format.
6. Select the time period over which the statistics should be created.
7. Click **OK**.

The user statistics are output in the selected format.




5.20.4 Generate report

Generate reports (page 64) about users, user groups, privileges, licenses, assignments, etc.

Prerequisite

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

Procedure


1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Generate report**. The corresponding dialog opens.
4. Select the relevant report.
5. Select the output format.
6. Click **Start**.
7. Click **OK**.

The report is output as an Excel file.




5.20.5 Generate License audit (password-protected) report

If your contract with Software AG contains a term under which you must regularly provide the usage data of the purchased licenses, generate the **License audit (password-protected)** report. This report is applicable to **Concurrent** and **Named user** licenses. For detailed information, contact your local Software AG sales organization (<https://www.softwareag.com/corporate/company/global/offices/default.html>).

Prerequisite

- You have the **User administrator**, **Configuration administrator**, and **License administrator** function privileges.
- **License monitoring** is enabled in  **Licenses > Monitoring > Configuration**.

Procedure


1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Generate report**. The corresponding dialog opens.
4. Select **License audit (password-protected)** report.
5. Click **Run**.

The report is output as a password-protected ZIP file containing an Excel file and a JSON file. Send this password-protected report to Software AG for evaluation.




5.20.6 Generate License usage rule validation report

Generate a report that lists the license usage based on the license rule. This report is applicable to **Concurrent** and **Named user** licenses.

Prerequisite

- You have the **User administrator**, **Configuration administrator**, and **License administrator** function privileges.
- License monitoring is activated (page 6) ( **Licenses > Monitoring > Configuration**).
- An active license rule is available (page 7) ( **Licenses > Monitoring > Rules**).

Procedure

1. Click  **User management**. The list of users is displayed.
2. Click  **Additional functions**.
3. Click  **Generate report**. The corresponding dialog opens.
4. Select **License usage rule validation** report.
5. Click **Run**.

The report is output as an Excel file.

5.20.7 Active sessions and history

USERS > <USER NAME> > ACTIVE SESSIONS

Obtain information on the time the user was logged in. This is where you can also log out the user (page 24).

USERS/USER GROUPS > <USER NAME/USER GROUP NAME> > HISTORY

Retrieve information on the events including their timestamp of a user/user group:

USERS

- User created
- User updated
- Privilege assigned
- User assigned to a group
- Synchronized with LDAP
- Login failed
- Password changed

USER GROUPS

- User group created
- User group updated
- Privilege assigned
- User assigned
- Synchronized with LDAP

5.20.8 ARIS Architect 'Administration' tab versus ARIS Administration

Users and privileges are managed centrally for all databases and ARIS products of an activated tenant. The role-dependent data access is controlled by access privileges and filters that are assigned per database in ARIS Architect on the **Administration** tab.

ARIS ADMINISTRATION

Centrally manage users, user groups, privileges, licenses, and configurations for all databases of a tenant. This ensures single sign-on for various ARIS products. Users can also be created using an LDAP system.

'ADMINISTRATION' TAB IN ARIS ARCHITECT

When you create a database, all users and user groups from the user management are automatically imported into the database. Administrators assign function and access privileges, as well as filters to users and user groups in each database so that only authorized users can view certain database content or perform specified actions. Use the prefix management to track which user created or changed database items.

ARIS video tutorial

ARIS Architect 'Administration' tab versus ARIS Administration

(<https://www.ariscommunity.com/videos/aris-architect-administration-tab-versus-aris-administration-0>) (approx. 1 minute)

5.20.9 Which reports exist?

You can generate the following reports as Excel files.

LICENSE AUDIT (PASSWORD-PROTECTED)

Lists the maximum consumption of each license per day.

USER GROUPS WITH ASSIGNED USERS AND PRIVILEGES

Outputs a list of the selected user groups and the users assigned to them, along with the function and license privileges granted to the user via the group.

ACTIVE USER SESSIONS

Outputs a list of all users currently logged in to ARIS, along with the start date and time of the session.

ASSIGNED AND UNUSED ARIS LICENSES

Outputs the total number of products and licenses, along with the number of licenses used and available.

LICENSE USAGE RULE VALIDATION

Based on the license rule specified, this report lists the license violations that occur in the system.

USERS WITH ASSIGNED PRIVILEGES

Outputs a list of the selected users with their assigned function and license privileges.

5.20.10 Delete and anonymize user accounts

Users can only be deleted (page 25) in ARIS Administration. To anonymize users in the different ARIS components according to GDPR, follow the instructions of the respective online help or manual:






- **ARIS Cloud Controller (ACC) Command-line Tool** manual
- **ARIS Server Administrator Command-line Tool** manual
- **ARIS document storage Command-Line Tool** manual
- **ARIS Process Governance Command-Line Tool** manual

- **User Management Command-Line Tool** manual
- **ARIS Risk & Compliance Manager online help > Procedures > Use ARIS Risk & Compliance Manager administration > Anonymize users** and **Specify anonymization patterns**
- **Collaboration > online help > Administrate Collaboration > How can user accounts be deleted and anonymized?**

After anonymization, users and their activities are shown with **Anonymized user** instead of with the user name.

5.20.11 What profiles include which content?

Profiles provide users a profile based view of the portal. Depending on the profile, the information and functionality that users have access to varies. Example: For users to which the **Viewer** profile is assigned, the **Steps** fact sheet is displayed when a model is selected. They are unable to view the **Tasks** fact sheet and the **Contribute** function as they do not have an active role. Profiles are applied in addition to the function (page 45) and license (page 48) privileges. If more than one profile is assigned, the user can switch between these profiles via **<user name> > Profiles > <profile_xy>**. Only one profile can be active at a time. You can assign (page 44) the following profiles to users or user groups in ARIS Administration.

Profile name	Views and functionalities
CoE member	The Overview fact sheet is displayed when a model is selected in  Published content .
Contributor	The Steps fact sheet is displayed when a model is selected in the Content view. If the Steps fact sheet is not available, the Overview fact sheet is displayed.
Designer	The Diagram fact sheet is displayed when a model is selected in  Published content .
Manager/Owner	The Dashboards fact sheet is displayed when a model is selected in  Published content .
Viewer	<ul style="list-style-type: none"> ▪ The Steps fact sheet is displayed when a model is selected in the Content view. If the Steps fact sheet is not available, the Overview fact sheet is displayed. ▪ The Tasks area is not available. ▪ The  Contribute function is not available.
Viewer (accessible)	<ul style="list-style-type: none"> ▪ The Steps fact sheet is displayed when a model is selected in the Content view. If the Steps fact sheet is not available, the Overview fact sheet is displayed. ▪ The Tasks area is not available. ▪ The  Contribute function is not available. ▪ ARIS document storage and Process Governance are not available.

These profiles are predefined in the XML configuration.




6 Configure jobs for ARIS document storage

You can configure jobs for ARIS document storage, which are executed regularly at a defined time.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click **Infrastructure**.
5. In the **Batch job schedule** field, enter the time at which a lock should be removed automatically. The time defined in the string must be a CRON expression (for example, '0 2 * * ?' if this is to happen every night at 2:00 a.m.).

You have defined the point in time at which the automatic jobs should be run.


7 Display charts for documents

You can display various charts for documents.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Open ARIS Connect and log in with your user name and password.
2. Click  **Charts**.
3. Click **Documents**.

The charts for documents are displayed.

8 Use ARIS document storage with WebDAV

ARIS document storage supports WebDAV. You can connect only one tenant with a specific repository.

To grant users without the **Document management** role access to ARIS document storage content, ARIS document storage can be used as a WebDAV network drive.

With a Microsoft® Windows 7 operating system you just need to connect the relevant network and access ARIS document storage directly. With older operating systems, you need to use Web folders (select **Tools > Map Network Drive > Sign up for online storage connect to a network server** in Microsoft® Windows Explorer). If this does not work, you must configure your computer as follows.

Procedure

1. Open the Registry Editor.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters** and find the DWORD entry **BasicAuthLevel**.
3. Check if the value of this entry is **2**. If the value of this entry differs, please change it to **2**. If the DWORD entry does not exist, create it.
4. With operating systems older than Microsoft® Windows 7 you also need to find the DWORD entry **UseBasicAuth**. If it does not exist, create it.
5. Change the value of this entry to the hexadecimal value **1**. Thus, you enable HTTP Basic Access Authentication for SSL and non-SSL connections.
6. Close the Registry Editor.
7. Restart Microsoft® Windows.

You can now use ARIS document storage as a WebDAV network drive.

9 Export statistics

You can export statistics for documents if **Generate usage statistics** is configured (page 290) for ARIS document storage.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click **Administrative actions**.
3. Click **Export statistics**. If you want to export all event types, enable the check box in front of **Event types**.

You can save the document statistics file of ARIS document storage at the relevant location for further use.

10 Use metadata

Metadata can be used to classify documents and is displayed in the properties (page 72) of a document.





10.1 Define custom metadata for documents

You can define custom metadata for documents saved in ARIS document storage. You can define attributes of type **String** or **Value**. If you define an attribute of type **Value**, you need to specify the allowed value range. For example, this user-defined metadata could be the color (green, blue, yellow) or the company size (small, medium, large). This metadata can be used to classify documents and is displayed in the properties (page 72) of a document.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click the arrow next to ARIS document storage.
3. Click  **Open properties**. The details (page 98) of the folder are displayed.
4. Click **Attribute types**.
5. Click  **Add new attributes**. The **Add attribute type** dialog opens. Add the relevant attribute type.

You have defined custom metadata.

A user-defined attribute type cannot be changed. You can add or delete values.





10.2 Delete custom metadata

You can delete custom metadata.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click the arrow next to ARIS document storage.
3. Click  **Open properties**. The details (page 98) of the folder are displayed.
4. Click **Attribute types**.
5. Move the mouse pointer over the attribute type to be deleted.
6. Click  **Delete**.

You have deleted custom metadata.



10.3 Display document properties

You can view the properties of a document or a folder.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click a folder in the navigation.
3. Click the relevant document. The **Document details** page opens.

The properties of the document are displayed.



10.4 Edit document properties

You can edit the properties of a document.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click a folder in the navigation.
3. Click the relevant document. The **Document details** page opens.
4. Edit the document properties, for example, change the description.
5. Click **OK**.

You have edited the properties of the document.



10.5 Generate a dashboard link

You can generate a link to a permanent document (page 83) located in ARIS document storage. This link can be used in data feeds or dashboards for ARIS Aware.

Prerequisite

- You have the **Dashboard administrator** function privilege.
- You have an ARIS Connect Designer (page 48) or ARIS Connect Viewer license.
- Your ARIS Server is enabled for ARIS Aware.

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click the document for which you want to generate a link to the document location in ARIS document storage.
3. Click **Show server location**.
4. Click **Copy to clipboard**.

The link to the document is copied to the clipboard and can be used in data feeds or dashboards for ARIS Aware.




10.6 Edit document tags

You can edit the tags of a document. You cannot edit an existing tag, you can only delete it and replace it with a new one.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click a folder in the navigation.
3. Click the relevant document. The **Document details** page opens.
4. Click  **Edit**.
5. Enter a new tag. You can separate multiple tags by a comma.
6. Click **Save**.

You have edited the tags of the document.




10.7 Delete tags of a document

You can delete the tags of a document.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click a folder in the navigation.
3. Click the relevant document. The **Document details** page opens.
4. Click  **Edit**.
5. Click the little cross beside the tag name.
6. Click **Save**.

You have deleted a tag.





10.8 Change the document owner

You can change the owner of a document.

Prerequisite

You have the **ARIS Connect Designer** license.

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click a folder in the navigation.
3. Click the relevant document. The **Document details** page opens.
4. Click  **Edit**.
5. Next to the **Owner** field, click  **Edit**. The **Select owner** dialog opens.
6. Enter a character string that is part of the user name of the new owner. The matching users are displayed.
7. Enable the relevant user.

You have changed the owner of a document.

11 Use folders

The folder structure of ARIS document storage provides a better overview and the possibility to specify access privileges (page 78).




11.1 Create folder in ARIS document storage

You can manage documents in your ARIS document storage. For a better overview, create a folder structure.

Prerequisite

You have the license right **ARIS Connect Designer** and have the corresponding permissions (**Document administrator**, **Local administrator**, or write permission).

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click a folder in the navigation.
3. Click the arrow next to a folder to open the menu.
4. Click  **Add folder**.
5. Enter a name for the folder, and click **OK**.

You have created a new folder.





11.2 Display folder details

You can view the details of a folder.

Prerequisite

You have the license right **ARIS Connect Designer** and have the corresponding permissions (**Document administrator**, **Local administrator**, or write permission).

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click the relevant folder, and click the arrow to open the menu.
3. Click  **More**.
4. Click  **Open properties**.

The details (page 98) of the folder are displayed.






11.3 Edit folder details

You can edit the properties of a folder.

Prerequisite

You have the license right **ARIS Connect Designer** and have the corresponding permissions (**Document administrator**, **Local administrator**, or write permission).

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click the relevant folder, and click the arrow to open the menu.
3. Click  **More**.
4. Click  **Open properties**. The details (page 98) of the folder are displayed.
5. Click  **Edit**.

You can edit the properties (page 98) of the folder.




11.4 Move folders in ARIS document storage

You can move folders in your ARIS document storage. The subfolders contained are also moved to the target folder.

Prerequisite

- You have the **ARIS Connect Designer** license privileges.
- You have access privileges (page 79) for the source folder and read and write privileges for the target folder.

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click a folder in the navigation.
3. Click the arrow next to a folder to open the menu.
4. Click  **Move to another folder**.
5. Select the folder and click **OK**.

You have moved a folder and its subfolders.

11.5 Manage folder access for user groups

By default, no access privileges are defined in ARIS document storage. All users have access to all folders - including the root folder - and documents. You can limit the access (page 82) to individual folders of ARIS document storage so that not all ARIS document storage users can access all folders and their contents.






Warning

If you edit the access of a user or a user group to a folder for the first time, you also must adapt the access privileges of the remaining users or user groups accordingly. Otherwise, all the remaining users or user groups will have no access at all.

Prerequisite


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

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click the relevant folder, and click the arrow to open the menu.
3. Click  **More**.
4. Click  **Open properties**.
5. Click **Access privileges**.
6. Click **Users groups**.
7. Enable the check boxes of the user groups whose access privileges you want to change.
8. Click  **Edit access privileges**. The **Edit access privileges** dialog opens.
9. Enable **Pass access privileges on to all subfolders** if users or user groups should have access to the subfolders below the selected folder. Select the relevant access privilege from the list.
10. Click **OK**.

You have restricted the access to ARIS document storage folders.

Tip

If you want to change the access privileges for a single user group, move the mouse pointer to the row of the relevant user group and click  **Edit access privileges**.

11.6 Manage folder access for users

By default, no access privileges are defined in ARIS document storage. All users have access to all folders - including the root folder - and documents. You can limit the access (page 82) to individual folders of ARIS document storage so that not all ARIS document storage users can access all folders and their contents.






Warning

If you edit the access of a user or a user group to a folder for the first time, you also must adapt the access privileges of the remaining users or user groups accordingly. Otherwise, all the remaining users or user groups will have no access at all.

Prerequisite


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

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click the relevant folder, and click the arrow to open the menu.
3. Click  **More**.
4. Click  **Open properties**.
5. Click **Access privileges**.
6. Click **Users**.
7. Enable the check boxes of the users whose access privileges you want to change.
8. Click  **Edit access privileges**. The **Edit access privileges** dialog opens.
9. Enable **Pass access privileges on to all subfolders** if users or user groups should have access to the subfolders below the selected folder. Select the relevant access privilege from the list.
10. Click **OK**.

You have restricted the access to ARIS document storage folders.

Tip

If you want to change the access privileges for a single user, move the mouse pointer to the row of the relevant user and click  **Edit access privileges**.





11.7 Show assigned users or user groups

You can restrict the view to those users or user groups who have access privileges to the selected folder.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click the relevant folder, and click the arrow to open the menu.
3. Click  **More**.
4. Click  **Open properties**.
5. Click **Access privileges**.
6. Click **Users** or **User groups**.
7. Enable **Show assigned users**.

Users or user groups who have access privileges to folders in ARIS document storage are displayed.






11.8 Exclude folder(s) from search

You can exclude ARIS document storage folders from the search.

Prerequisite

- You have the **ARIS Connect Designer** license privileges.
- You have read and write privilege for the relevant folders.

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click the relevant folder, and click the arrow to open the menu.
3. Click  **More**.
4. Click  **Open properties**.
5. Click  **Edit**.
6. Enable **Exclude from search**.
7. Click **Save**.

You have excluded folders from the search. If you search for documents that are located in the excluded folder, no document is found. Only the folders not excluded are searched through. This has no effect on the subfolders of the excluded folder.




11.9 Delete folder in ARIS document storage

You can manage documents in your ARIS document storage. For a better overview, create a folder structure.

Prerequisite

You have the license right **ARIS Connect Designer** and have the corresponding permissions (**Document administrator**, **Local administrator**, or write permission).

Procedure

1. Click  **Application launcher** >  **Documents**.
2. Click a folder in the navigation.
3. Click the arrow next to a folder to open the menu.
4. Click  **Delete**. The **Confirmation** dialog opens.
5. Click **OK**.

You have deleted the folder.

12 Good to know

This section provides background information to assist you in carrying out the relevant procedures.

12.1 What is ARIS document storage?

ARIS document storage is a repository where documents can be stored temporarily or permanently to use them, for example, to specify objects and models and as a basis for displaying dashboards.

Access restriction on folder level is possible in ARIS document storage.

The documents saved there can be used during runtime of an executable process, for example, attached to an e-mail.

All file formats are allowed for documents.

Temporary documents (page 83) are deleted automatically after the executable process is terminated. Permanent documents (page 83) are kept until they are deleted explicitly.

You can work with documents in the repository or in the portal.

12.2 Access privileges for folders

By default, no access privileges are defined in ARIS document storage. All users have access to all folders - including the root folder - and documents. You can limit the access to individual folders of ARIS document storage so that not all ARIS document storage users can access all folders and their contents. The following access privileges exist:

- All access privileges

The users or user groups with this privilege have full access to the folder and can view, edit, create subfolders and delete the folder but cannot assign privileges to users or user groups. They can upload new documents, new document versions, and delete documents.

- Folder administration access

The users or user groups members with this privilege are local administrators for the folder and can view, edit, create subfolders, delete the folder, and assign privileges to the users and groups. But they cannot assign the **Folder administration access** privilege to other users or user groups. They can upload new documents, new document versions, and delete documents.

When the **Folder administration** access privilege of a folder is revoked, the user also loses the **Folder administration** access privilege for all the subfolders that have implicit pass-on behavior. Thus, if no other restrictions apply, all users have access to these folders again.

- Reset access privileges

The users or user groups with this privilege can revoke the permission on the folder if already assigned.

- 'Read' access privilege

The users or user groups with this privilege can view the folder but are unable to upload new documents and new document versions or delete documents in the folder nor create new subfolders.

- 'Read + Write' Access privilege

The users or user groups with this privilege can view and edit the properties of the folder and create subfolders. They can upload new documents, new document versions, and delete documents.

12.3 Permanent documents

Permanent documents remain in the ARIS document storage until they are explicitly deleted.

You can set up (page 78) access restrictions on the folder level for permanent documents.

If you use Process Governance, it is recommended that you specify that documents are to be saved permanently in ARIS document storage when modeling a dialog for an executable process, otherwise the location for these documents within ARIS document storage cannot be specified in the dialog. These documents are called temporary documents (page 83).

You can restrict access privileges on folder level only, not for individual documents. Users having the **Document administrator** function privilege can access all folders. If no roles are defined for access to a folder, all users have access to it.



12.4 Temporary documents



Temporary documents are documents that were not explicitly uploaded to ARIS document storage but were added to the process during process instance runtime if you use Process Governance. They can be transformed into permanent documents and added to ARIS document storage if required.



Temporary documents are also saved in the safe area of ARIS document storage when you use an external document management system. These documents are deleted when the process instance is terminated.



You can transform a temporary document into a permanent document by moving it to ARIS document storage.

12.5 Options for models or objects

There are two options to connect documents with an object or model: The first is using the **ARIS document storage** attribute of an object or model. In the document details, documents connected with an object are preceded by the  symbol, and documents connected with a model are preceded by the  symbol.

The second option is to assign documents to an object or model in ARIS Connect Designer. The assignment is marked by the  link symbol for objects and  for models.

In this case, the document details show that this document is connected via attributes with an object () or a model ()

The second option includes direct attachment to an object or model in ARIS Connect Designer. This is marked by the  or  link symbols.

12.6 External document management systems

This is where permanent documents (page 83) are managed. The storage for temporary documents (page 83) is not affected by this.

Available is Microsoft® SharePoint 2013.

12.7 Folder Dashboarding

Data is collected by scheduled reports (page 86) and form the basis for data feeds that are stored in the **Dashboarding** folder in ARIS document storage.

These reports generate XML files.

By default, all users have access to the **Dashboarding** folder. Therefore, it is strongly recommended that you restrict the access (page 78) to the **Dashboarding** folder and all its subfolders to the user that is configured in the URL alias (page 390).

The **United Motor Group** database is supplied with your ARIS installation by default. With this database, you receive a set of default dashboards that can be displayed within ARIS Connect.

By default, at least the following folders are available in the **Dashboarding** folder:

- Collaboration - containing the dashboards for Collaboration
- Governance - containing the dashboards for Process Governance
- Matomo - containing the dashboards collected by Matomo

Under United Motor Group folders

- CoE - containing the dashboards for Center of Excellence
- CXM - containing the dashboards for Customer Experience Management
- EA - containing the dashboards for Enterprise Architecture
- Exported Tables - containing the dashboards for metadata, for example, for the person responsible for a process
- GRC - containing the dashboards for Governance, Risk & Compliance (GRC)
- IoT - containing the dashboards for Internet of Things
- Matomo - containing the dashboards collected by Matomo from the **United Motor Group** database
- PPM - containing the dashboards for ARIS Process Performance Manager
- SAP - containing the dashboards for ARIS for SAP® Solutions
- Strategy - containing the dashboards for Business strategy

12.8 Scheduled reports

Scheduled reports are reports that start automatically at a defined point in time.

They run in the background and you can view the results later. For example, you can define that a report that strongly affects system performance is to run only at night when no one is working with the system.

You specify the schedule for reports in ARIS Architect. For further information please refer to the **Evaluate data > Use reports > Create schedule for report** chapter of the ARIS Architect online help.

12.9 Charts for documents

12.9.1 'Number of documents' chart

This chart only displays information.

It shows the total number of all documents per repository in ARIS document storage, if multiple repositories exist. Otherwise, the total number of documents is displayed.

12.9.2 'Used space' chart

This chart is a speedometer display.

If memory space (in kilobyte) for ARIS document storage for a tenant is restricted, the memory used is shown in the form of a speedometer. If no maximum memory space has been defined, the memory used is shown in megabytes.

12.9.3 'Most viewed documents' chart

This chart is a bar chart.

It shows the 15 most viewed or downloaded documents including their file size.

12.9.4 'Most changed documents' chart

This chart is a bar chart.

It shows the 15 most changed documents including their file size.

12.9.5 'Largest documents' chart

This chart is a bar chart.

It shows the 20 largest documents including their file size.

12.9.6 'Latest documents' chart

This chart is a simple list.

This chart shows the 15 latest documents.

12.9.7 'Document status overview' chart

This chart is a pie chart.

It shows the distribution and number of documents in the various document statuses.

Document statuses are **In progress**, **Under review**, **Reviewed**, **Rejected**, and **Published**.

12.9.8 'Outdated documents' chart

This chart is a simple list.

This chart shows the 15 oldest documents.

12.10 Delete and anonymize user accounts

Users can only be deleted (page 25) in ARIS Administration. Then, they must be anonymized according to GDPR. Users are anonymized either with `y-admintool.bat` for Windows operating systems or `y-admintool.sh` for Unix operating systems. For detailed information, refer to **ARIS document storage Command-Line Tool**.

After anonymization, activities of ARIS document storage users, such as uploads of documents, downloads of documents, changes to metadata, are shown with **Anonymous** instead of with the user name.

13 Pages in ARIS document storage

13.1 ARIS document storage attribute types

Enables the definition of custom metadata for documents saved in ARIS document storage. This page is available only for the root folder.

GENERAL BUTTONS

Add new attributes

Opens the **Add attributes types** dialog in which you can enter new attribute types for documents.

TABLE

Key

Specifies the key of the attribute. This is the name that is displayed in front of the box of allowed values.

Type

Specifies the type of the attribute.

Value range

Specifies the values that a user-defined attribute may have.

Edit

Opens the **Change attribute type** dialog. This is only available for attributes of the **Value** data type.

Delete

Deletes a value from the list of allowed values for an attribute of the **Value** type.

13.2 Document details

Displays document details.

GENERAL BUTTONS

Buttons on the top right, whose functionality applies to the entire document including its versions.

Upload new version 

Download 

Lock 

Unlock 

Delete 

Edit 

Enables the editing of a document.

TABLE

File name

Displays the name of the document.

Path

Displays the path to the document.

Title

Displays the title of the document.

Current version

Displays the current version of the document. During a new upload of the document the last number is increased. When the document status is changed, the number in the middle is increased. The states **New**, **Approved**, **Rejected**, **In process**, and **To be approved** exist.

Revision

Shows the number of the revision for the selected document. Each time a document is checked out and changed, a new revision number is assigned.

Status

Shows the status of the document. The states **New**, **Approved**, **Rejected**, **In process**, and **To be approved** exist.

ID

Displays the ID of the document.

File size

Displays the size of the file.

Owner

Displays the name of this document's owner.

Locked by

Displays who has opened or locked the selected document.

Created by

Displays who created the document in ARIS document storage.

Created on

Displays the creation date of the document.

Description

Displays a detailed description of the document if the description is specified.

List of tags

Displays tags, if they exist. You can add new tags and edit or delete existing ones.

Link

Displays the link to the physical location.

Optional: Custom metadata

Displays the custom metadata, if defined.

13.3 Document history

Displays the history of a document.

GENERAL BUTTONS

Buttons on the top right, whose functionality applies to the entire document including its versions.

Upload new version 

Download 

Lock 

Unlock 

Delete 

TABLE

Timestamp

Shows the timestamp of the change to a document to the second, as well as the date of the change.

User name

Shows the user name that the user who performed the change was logged in with.

Event

Shows the change made, for example, an update of the document relationship or a change to a document's metadata.

Details

Shows the event in detail.

13.4 Document relations

Displays the relationships of a document.

GENERAL BUTTONS

Buttons on the top right, whose functionality applies to the entire document including its versions.

Upload new version 

Download 

Lock 

Unlock 

Delete 

TABLE

Type

Shows the type of the relationship, for example, **ARIS_Model**, if the document is directly connected to a model. The following relationship types are displayed:

- The document is connected to a model via a link (**ARIS document storage** attribute type group)
- The document is connected to an object via a link (**ARIS document storage** attribute type group)
- The document is connected directly to a model (**ARIS_Model**)
- The document is connected directly to an object (**ARIS_OBJECT**)

Reference

Shows the document's reference to a model or object. The GUID of the model or object is shown, as well.

Delete

Deletes the relation of the document.

If, for example, the document is connected with a model, this relationship is deleted from the model.

A confirmation prompt is shown. Click **OK** to delete the relation. If you decide not to delete the relation, click **Cancel**.

13.5 Document versions

Displays the versions of a document.

GENERAL BUTTONS

Buttons on the top right, whose functionality applies to the entire document including its versions.

Upload new version 

Download 

Lock 

Unlock 

Delete 

TABLE

Revision

Shows the number of the revision for the selected document. Each time a document is checked out and changed, a new revision number is assigned.

Size

Displays the size of the file.

Changed on

Shows the date a document version was changed.

Changed by

Shows which user changed a version of a document.

Comment

Shows the comment entered when changing the version of the document.

Status

Shows the status information of the document. The following status information is possible:

- NEW
- ON_APPROVAL
- IN_PROGRESS
- APPROVED
- REJECTED

- PUBLISHED

VERSION-SPECIFIC BUTTONS

If you move the mouse pointer to the row of a version the version-specific buttons are displayed.

Open version 

Delete 

13.6 Folder access privileges for user groups

Displays the folder access privileges of the associated user groups.

GENERAL BUTTONS

Delete 

Deletes the selected folder, its subfolders and all documents in them.

Enter search term field

Enter the name of the user group or user you want to edit.

Pass on access privileges to all subfolders

Activates the function based on which the restriction of access privileges is extended to all subordinate folders of the selected folder.

TABLE

User group name

Displays the name of the user group.

Access type

Displays the access privilege of a folder for a user group or a user.

Edit

Opens the **Edit access privileges** dialog.

13.7 Folder access privileges for users

Displays the folder access privileges assigned to users.

GENERAL BUTTONS

Delete 

Deletes the selected folder, its subfolders and all documents in them.

Enter search term field

Enter the name of the user group or user you want to edit.

Pass on access privileges to all subfolders

Activates the function based on which the restriction of access privileges is extended to all subordinate folders of the selected folder.

TABLE

User name

Displays the name of the user.

Full name

Displays the full name of a user.

Access type

Displays the access privilege of a folder for a user group or a user.

Edit

Opens the **Edit access privileges** dialog.

13.8 Folder

Displays the content of a folder.

GENERAL BUTTONS

Upload

Opens the dialog to upload a new document.

Refresh

Refreshes the page displayed.

TABLE

Name

Displays the name of the document.

File type

Displays the file type of the document.

Status

Shows the status of the document. The states **New, Approved, Rejected, In process,** and **To be approved** exist.

Upload new version

Shows the status of the document. The states **New, Approved, Rejected, In process,** and **To be approved** exist.

Download

Shows the status of the document. The states **New, Approved, Rejected, In process,** and **To be approved** exist.

Open properties

Opens the properties of the document.

Move to another folder

Opens the **Move document** dialog.

Delete

Deletes the document from ARIS document storage.

13.9 Folder details

Displays the details of a folder. (page 76)

GENERAL BUTTONS

Delete

Deletes the selected folder, its subfolders and all documents in them.

Edit

Enables editing mode for the folder details.

TABLE

Folder name

Displays the name of the folder.

Path

Displays the path to the folder.

ID

Displays the ID of the folder.

Created by

Displays who created the folder in ARIS document storage.

Created on

Displays the creation date of the folder.

Exclude from search

Enables that folders are excluded from the search. If you search for documents that are located in the excluded folder, no document is found. Only the folders not excluded are searched through. This has no effect on the subfolders of the excluded folder.

13.10 Folder history

Displays the folder history.

GENERAL BUTTONS

Delete

Deletes the selected folder, its subfolders and all documents in them.

Refresh

Refreshes the page displayed.

TABLE

Timestamp

Displays the timestamp of the changes to the folder details.

User name

Displays the user who changed the folder details.

Event

Displays what changes were made to the folder, for example, the creation of a new subfolder.

Details

Displays a detailed comma-separated list of the changes made to the folder.

13.11 Select document page

Enables selection of the documents you want to add. Multiple selection is possible.

Double-click to add a single document to the selection.

ARIS document storage

Enables you to select a document that is stored in ARIS document storage.

Microsoft® SharePoint 2013

Enables you to select a document that is stored in a third-party document management system.

Properties

Opens the **Document properties** dialog. This dialog displays document properties, such as file name, version, and file type.

Previous version

Opens the **Document versions** dialog, which displays a list of document versions with the corresponding change list numbers, the change date, and the name of the editor.

Add to selection

Adds the selected document to the document selection.

Clear selection

Clears the selection. All documents are removed from the selection.

Remove document

Removes the selected document from the selection. Multiple selection is possible. Select adjacent documents by holding down the Shift key and clicking the first and last document. Select individual objects by holding down the Shift key and clicking the relevant documents.

EXPLORER TAB

Click the small right arrow in order to navigate to further subfolders.

Selected documents

Displays the list of documents already included in the selection.

SEARCH TAB

Find what

Enables you to enter a term that occurs in the title, file name, description, or tags of the document.

Search result

Displays the documents that match the search criteria.

Selected documents

Displays the list of documents already included in the selection.

13.12 Select tags page

From the available tags, select those you want to use for marking the document.

Specify tag filter...

Used for entering a search term to restrict the number of the tags displayed existing in the system. When you enter the first letters the display is restricted to the tags that fit your input.

Select tags to be added

Enable the check box in front of the tags you wish to identify the document with.


13.13 Upload document page

Enables the upload of the required document.

File

Enter the name of the file. To search your file system, click  **Browse**.

Location

Enables you to select the location where files are to be saved in ARIS document storage. Click the small right arrow in order to navigate to further subfolders. To browse, click  **Browse** next to the box.

Comment

Enables you to enter a comment that will be displayed in the **Document versions** dialog.

Title

Used to enter the title of the document to be uploaded.

Description

Used to enter the description of the document to be uploaded.


Tags

Displays tags, if they exist. You can add new tags and edit or delete existing ones.

Enter suggestions here

Used to enter new tags. Press Enter to transfer the new tag.


Delete individual tag

Click  **Delete** to delete an individual tag or selected tags for this document. Multiple selections are allowed.

Delete all tags

Click  **Delete all tags from list** to delete all tags for this document.

Find

Click  **Find** to search for corresponding tags for this document in your ARIS document storage.

14 Administrate automated processes

Process administration (page 103) in ARIS Connect provides information and functions pertaining to automated processes.

ARIS video tutorial


14.1 Open process administration

You can perform different actions in process administration and retrieve information.

Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. ARIS Administration opens.
2. Click  **Process administration**.

The functions and information of process administration are available.

Depending on whether you select **Processes**, an executable process, a version, or a process instance of an executable process, different information and functions are displayed.

ARIS video tutorial

Process administration overview

(<http://www.ariscommunity.com/videos/process-administration-aris-connect-overview>)

(approx. 4 minutes)

14.2 What is 'Process administration' used for

Process administration provides information about executable processes as well as control and error handling functions (page 110). You need the **Process Governance administrator** function privilege.

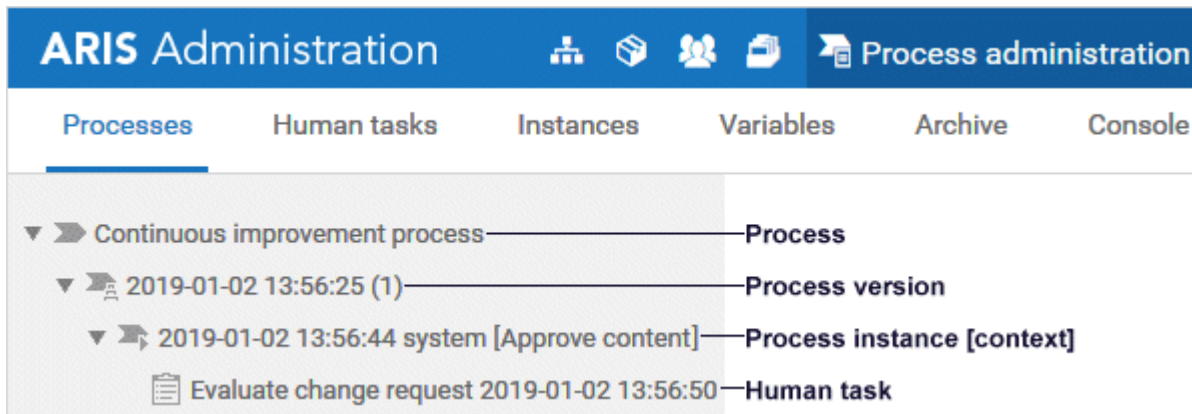
Warning

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)

Depending on the selected process level and menu item, various information and functions are available.

Process levels



The superordinate menu items display information for all processes. The menu items in the information area apply only to the selected process.

ARIS video tutorial

Process administration overview

(<http://www.ariscommunity.com/videos/process-administration-aris-connect-overview>)

(approx. 4 minutes)

Find and correct problems in processes



(<http://www.ariscommunity.com/videos/learn-how-find-problems-process-and-correct-processes>) (approx. 4 minutes)



14.2.1 What does 'Activities' provide?

Activities are displayed if you have selected a process instance of an executable process. It displays the activities of the executable process of the **BPMN process diagram (BPMN 1.x)** type. To skip (page 124) an activity, move the mouse pointer over the relevant row, and click

▶ **Skip activity.**


14.2.2 What does 'Archive' and 'Archive history' provide?

The archived instances (page 118) are listed. Use  **Show/hide filter** to restrict the number of process instances displayed according to various criteria. You can export the data as a CSV file (.

To unarchive instances, move the mouse pointer over the relevant table row and click  **Unarchive selected instances**. To permanently delete archived instances, move the mouse pointer over the relevant table row and click  **Delete**.

To suspend archiving, unarchiving, or deletion, click **Suspend** in the progress dialog. Alternatively, you can use the suspend function in **Archive history**. Please note that operations that have been already completed are not reverted. Example: An operation is running to archive ten instances. You suspend the operation after three instances have already been archived. Only the seven remaining instances are not archived.

To resume the operation, open **Archive history**, click **Resume** in the row of the previously suspended archiving execution. This is also helpful if an operation was suspended automatically, for example, during a backup.


Click **Archive history** to display the list of archiving executions (**ARCHIVING, UNARCHIVING, DELETE**). You can export the data as a CSV file (.

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)

14.2.3 What does 'Assignments' provide?

Assignments display the assigned users for a human task. To delegate (page 130) a human task, move the mouse pointer over the relevant task, and click  **Delegate task**.

14.2.4 What does 'Console' provide?

The console can be shown for all processes or for a process instance. The following messages are displayed:

- Log messages for process instance execution.
- Messages that were generated by the user interface during execution of process instances (log, server, and user management messages). You can filter the messages by their severity.

You can export the data as a CSV file (.

14.2.5 What does 'Context' provide?

The context and the process settings can be displayed for the process version or the process instance. The execution context determines from which items (database, group, model/object type, document), in which applications (for example, ARIS Connect), and by which users a governance process can be started. You must specify the context before generating the executable process. After this, it can no longer be changed for the generated process version. If no execution context is defined, the governance process can be started for all items (**Without context** option). The defined execution context is displayed in process administration. The context selected for the process instance is displayed in the navigation tree (page 103) and in Instances (page 108).

14.2.6 What does 'Details' provide?

Details (page 128) provide different information, such as ID, status, priority, depending on whether you selected a process, a process version, process instance, or a human task.

14.2.7 What does 'Diagram' provide?

Diagram is displayed if you have selected a version of an executable process or a process instance of an executable process. Use **Toggle between EPC and BPMN diagram** to toggle between the EPC display of the executable process and the BPMN diagram generated by the automatic model transformation.

Activities that are currently running or have failed are selected in both models (EPC and BPMN diagram). Compared to the EPC, the BPMN diagram can contain additional activities as these are required for the technical process. In this case, the last selected activity remains selected in the EPC until the next matching activity is reached.

All processes involved are displayed for executable processes that consist of multiple processes.

- If nothing is active, the start model is displayed.
- If an object is active, the models containing active objects are displayed.

To display the properties of the running activity, click the  **Show details** button.

14.2.8 What does 'History' provide?


History is displayed if you have selected a process instance of an executable process.

Activities run by process instances are listed. If an entry contains a process instance with the **Failed** status, the activity can be restarted (page 123) from here.



To display the input/output data or the simulation data for simulated activities, click the activity in the table.


To get additional details of an input activity, you can display the corresponding activity in the history table. In the row of the relevant input activity, click **Show associated activity in the history**. Alternatively, you can click **Used by** so that all activities for which the selected activity acts as an input activity are displayed.


Click **Input variables** or **Output variables** to show the values read (input) or stored (output) during execution of an activity.



Click **Input data** or **Output data** to check the data. Additionally, you can click  **Show details** to display the XML data. For restartable failed activities the tracking ID is displayed.

14.2.9 What does 'Human task' provide?



The human tasks of all executable processes are displayed. Use  **Show/hide filter** to restrict the number of process instances displayed according to various criteria. You can sort the table by different columns, for example, by status. You can export the data as a CSV file (.

To display a specific instance/version, move the mouse pointer over the relevant table row and click  **Display process instance** or  **Display process version**.



To display (page 130) detailed information about a specific human task, move the mouse pointer over the relevant human task, then select  **Show details**. Here, you can send (page 114) a reminder to the executors. To check the assigned users and delegate (page 130) a human task, click **Assignments**.



Statistics data in the form of charts (page 137) for human tasks are available under  **Application launcher** >  **Administration** > **Charts** > **Governance** > **Human tasks**.




14.2.10 What does 'Instances' provide?




It provides an overview of the process instances and their various statuses (page 133). Use  **Show/hide filter** to restrict the number of process instances displayed according to various criteria. You can sort the table by different columns, for example, by status. You can export the data as a CSV file (.

You can check if process instances failed so that you can correct (page 127) and restart them, if required.

To display a specific instance/version, move the mouse pointer over the relevant table row and click  **Display process instance** or  **Display process version**.

To archive instances that have the status (page 133) **Completed**, enable the relevant instances () and click  **Archive selected instances**.

To prioritize/deprioritize multiple instances simultaneously, open **Instances**, enable the relevant instances () and click  **Increase priority**/ **Decrease priority**. The function is only available if all selected instances meet the prerequisites for prioritization.



Statistics data in the form of charts (page 137) for Governance processes are available under  **Application launcher** >  **Administration** >  **Charts** > **Governance** > **Processes**.

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)

14.2.11 What does 'Variables' provide?

The variables can be shown for all processes, for a process version, or for a process instance. The variables used and their values are listed. You can export the data as a CSV file (). To display the XML data of the variable value, click a variable in the table. To show the previous values of a variable including their timestamps, click **History**. Additionally, you can show the values read (input) or stored (output) during execution of an activity. Once you selected a variable in the table, you can use  **Show details** to display or hide **Value as XML** and **History**.

14.3 Tasks of the Process Governance administrator

The Process Governance administrator manages the executable processes. Process administration provides information about executable processes as well as control and error handling functions (page 110). Depending on the selected process level and menu item, various information and functions are available.

- Start (page 111) governance processes in process administration, for example, older versions of the process.
- Deactivate (page 116) executable processes.
- Restart (page 123) activities in the status **FAILED**.
- Suspend/resume (page 114) the execution of process instances.
- Terminate (page 115) the execution of process instances if, for example, the executable process is no longer relevant.
- Prioritize and deprioritize (page 119) process instances
- Use the process instance archive (page 118) to improve performance.
- Configure recurrences for an executable process.
- Suspend/resume (page 115) the recurrence of an executable process.
- Suspend the recurrence of an executable process
- Resolve error in process.
- Read privileges for the Console (page 106) bar also at the process level.
- View all tasks of other users in **My tasks**.

Statistics data in the form of charts (page 137) for Governance processes are available under

 **Application launcher** >  **Administration** >  **Charts** > **Governance** > **Processes**.



14.4 Find process instances

Find process instances that have a certain status or property.

Prerequisites

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click **Instances**. The list of process instances is displayed.
3. Click  **Show/Hide filter**. The filter criteria are displayed.
4. Enable () the relevant filter criteria, for example, the **QUEUED** status (page 112). You can combine different filter criteria.
5. Click **Apply filter**.

The list of process instances that match the selected filter criteria is displayed.



14.5 Start governance process in process administration

You can start the executable process in process administration for processes or process versions.

Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Navigate to the executable process you want to start, or to the process version.
3. Under **Processes**, click the relevant process or process version.
4. Click  **Start governance process**. The **Select context** dialog opens. The items are displayed on which the executable process can be started depending on the specified execution context.
5. Select the relevant model. To select multiple models, hold down the **Ctrl** key and click the required models one after the other.
6. Click **OK**.

The governance process is started for the selected item.

14.6 Where can the executable process be started?

The executable process can be started in ARIS Architect, ARIS Designer, ARIS Connect, or in the ARIS Connect process administration. The message displayed after starting the governance process can be specified individually for each process (EPC, VACD).

14.7 What is an executable process?

An executable process is a process that reflects a certain process flow in your company with all the related steps. All information relevant to Process Governance is recorded in EPCs, value-added chain diagrams, organizational charts, dialogs, and data flows (BPM process). The BPM process is automatically transformed into a technical process that can be executed by Process Governance. All relevant information for the BPM process is interpreted, transformed into a BPMN diagram, and all relevant models and objects are archived. The BPMN diagram is the basis for Process Governance. It controls the governance process. The executable process can then be started for a specified context.


14.8 Context for executable processes

The execution context determines from which items (database, group, model/object type, document), in which applications (for example, ARIS Connect), and by which users a governance process can be started. You must specify the context before generating the executable process. After this, it can no longer be changed for the generated process version. If no execution context is defined, the governance process can be started for all items (**Without context** option). The defined execution context is displayed in process administration.

14.9 How many process instances can be started?

The number of process instances that can be processed in parallel by the engine is limited to 1000 per Process Governance node by default (**Configuration > Process Governance > Infrastructure > Batch processing size**). However, depending on the workflow complexity, it can be necessary to reconfigure this number, for example when using

- Custom report scripts or local services
- High number of parallel branches
- Deeply nested branches
- Large number of activities per instance
- Many task assignments per task (users/user groups)



The process instances have the **RUNNING** status. If the specified batch processing size is reached, the process instances started additionally have the **QUEUED** status. You can display (page 111) them in **Instances**. This  **Cross-tenant** setting applies to all tenants on this server. To change it, use ARIS Cloud Controller. For further information, refer to **ARIS Cloud Controller (ACC) Command-line Tool** manual.

Archive completed process instances regularly to avoid a large number of instances that can have a negative effect on runtime and start times in process administration and Process Governance.

14.10 Export process administration content as a CSV file

You can export data of **Human tasks** (page 107), **Instances** (page 108), **Variables** (page 109), **Archive** (page 104), or **Console** (page 106), for example, for evaluation purposes.

Procedure



1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click **Human tasks**, **Instances**, **Variables**, or **Console**, or go to **Processes** and click the process instance and then **History**.
3. Click  **Export as a CSV file** in the navigation bar. The corresponding dialog opens.
4. Select the output options.
5. Click **Export**.

The content is exported as a CSV file.



14.11 Send reminder about executing human task

You can send reminders about human tasks to the relevant executors.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Open the relevant human task.
3. Click  **Send reminder**.

The users assigned to the human tasks as executors receive an e-mail with the information that the task is to be edited.

If 75% of the processing time has expired, the executors automatically receive a reminder. If the task is not edited by the due date the escalation manager (page 121) is notified. Statistics data in the form of charts (page 137) for human tasks are available under  **Application launcher** >  **Administration** > **Charts** > **Governance** > **Human tasks**.

ARIS video tutorial



Process administration overview

(<http://www.ariscommunity.com/videos/process-administration-aris-connect-overview>)
(approx. 4 minutes)

14.12 Suspend/resume execution of process instance


You can suspend the execution of a process instance. This can be useful, for example, if a server outage would cause the process execution to fail.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the relevant process instance under **Processes**.
3. Click  **Suspend**.

The execution of the process instance is suspended. It has the status **Suspended**.



4. To continue it, click  **Resume**.

Unlike the  **Suspend recurrence** function, it is not the creation of recurrences that is suspended for the entire process, but only the execution of this process instance.



Example

The **Save data** process is started at midnight each night. The process comprises the two steps **Copy data** and **Archive data**.

- **Suspend recurrence**

If  **Suspend recurrence** is selected, the process will no longer be started as of the next night and will not resume until  **Resume recurrence** is selected. However, all running process instances are completed.



- **Suspend process instances**

If  **Suspend** is selected at night for a running process instance that has just finished copying data, this specific process instance is suspended, in other words, the data will no longer be archived. Process execution stops at this point. The next night, however, a new instance of the process is started, and the data is backed up and archived. The suspended process instance will not continue to run until  **Resume** is selected.

14.13 Terminate execution of process instance


You can terminate the execution of a process instance permanently if, for example, the executable process is no longer relevant.

Procedure




1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the relevant process instance under **Processes**.
3. Click  **Terminate**.


The execution of the process instance is terminated permanently.

14.14 Suspend/resume recurrence for executable process

You can suspend the recurrence of an executable process and resume it later. Processes for which a recurrence has been configured in ARIS Architect are identified in process administration by the symbol .

Procedure



1. Open (page 103)  **Process administration** in ARIS Connect.
2. In the navigation, click the relevant process version under **Processes**.
3. Click  **Suspend recurrence**.
The recurrence is suspended.
4. To continue it with the existing configuration, click  **Resume recurrence**.

Unlike the  **Suspend** function, the creation of recurrences is suspended for the entire process, not just for the execution of a given process instance.



Example

The **Save data** process is started at midnight each night. The process comprises the two steps **Copy data** and **Archive data**.

▪ Suspend recurrence

If  **Suspend recurrence** is selected, the process will no longer be started as of the next night and will not resume until  **Resume recurrence** is selected. However, all running process instances are completed.

▪ Suspend process instances

If  **Suspend** is selected at night for a running process instance that has just finished copying data, this specific process instance is suspended, in other words, the data will no longer be archived. Process execution stops at this point. The next night, however, a new instance of the process is started, and the data is backed up and archived. The suspended process instance will not continue to run until  **Resume** is selected.

14.15 Delete executable process

You can deactivate the executable process if, for example, this process is outdated and should therefore no longer be used.



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)

When a generated executable process is deactivated, the process version and all related information, such as instances, subprocesses, etc., are removed from process administration. The deactivated processes are not exported to ARIS Process Performance Manager.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Under **Processes**, click the process, process version, or process instance.
3. Click  **Delete**.

The selected item is deactivated.






14.16 Suspend, resume, or terminate simulation runs

You can suspend and resume active simulation runs or terminate them. This can be useful, for example, if a server outage would cause the process execution to fail.

Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the relevant process instance under **Processes**. Processes versions for which a Process Governance Simulation was performed are marked with , simulation runs and process instances with .
3. To suspend a simulation run, click the relevant process instance and select  **Suspend**.
4. Use  **Resume** to continue the simulation run at a later time.

- To stop a simulation run, select  **Terminate**. The simulation run is terminated and cannot be restarted.

The simulation run is suspended, resumed, or terminated depending on the selected action.

14.17 Use process instance archive

Archive completed process instances regularly to avoid a large number of instances that can have a negative effect on runtime and start times in process administration and Process Governance. Archiving instances gives you the following advantages:

- Process Governance starts faster.
- The process runtime is reduced.
- A better overview of your process instances.

You can only archive instances that have the status (page 133) **Completed**.

During archiving, the data of the corresponding instances is moved from the Process Governance database to an archive entry of ARIS document storage. Each tenant has its own archive. The information about simulation, recurrence, and substitution is not archived. If you want to automatically archive process instances, for example every night at a certain time, write a report in ARIS Script

([../..../..../..../abs/help/en/script/ba/index.htm#scripthelp.html](#)) and schedule it. This is done in ARIS Architect ([../..../..../..../abs/help/en/handling/ba/index.htm#72345.htm](#)).

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)

Prerequisites



- You have the Process Governance administrator (page 110) function privilege.
- The instances have the **COMPLETED** status (page 133).

Procedure


- Open (page 103)  **Process administration** in ARIS Connect.
- Click **Instances**. The list of process instances is displayed.
- Click  **Show/Hide filter**. The filter criteria are displayed.
- Enable () the **COMPLETED** status.

5. Click **Apply filter**. The list of completed process instances is displayed.
6. Enable () the instances to be archived. You can archive a maximum of 100 instances in one step.
7. Click  **Archive selected instances**. (The function is only available if at least one instance is enabled.)

The instances are removed from the **Instances** (page 108) list and are displayed in the **Archived instances** (page 104) list.


8. To move instances back from the archive to the **Instances** list, open the **Archived instances** list, move the mouse pointer over the relevant table row, and click  **Unarchive archived instances**.
9. To permanently delete archived instances, open the **Archived instances** list, move the mouse pointer over the relevant table row and click  **Delete**.
10. To suspend archiving, unarchiving, or deletion, click **Suspend** in the progress dialog. Alternatively, you can use the suspend function in **Archive history**. Please note that operations that have been already completed are not reverted. Example: An operation is running to archive ten instances. You suspend the operation after three instances have already been archived. Only the seven remaining instances are not archived.
To resume the operation, open **Archive history**, click **Resume** in the row of the previously suspended archiving execution. This is also helpful if an operation was suspended automatically, for example, during a backup.

Your operations were performed.

Alternatively, you can archive all completed instances of a process version. To do so, click the relevant process version under **Processes**, then click  **Archive all completed instances**. The archiving functionality can affect the total runtime and size of the backup.

14.18 Prioritize and deprioritize process instances





For each tenant there is a queue of process instances waiting to be executed. Each newly started process instance is appended to the end of the queue according to the first in, first out principle. However, you can prioritize process instances so that they are preferably executed.

The priority queue is limited to 100 process instances by default (**Configuration > Process Governance > Infrastructure > Priority queue size**). If the specified priority queue size is exceeded, so that no further process instances can be prioritized, a message is displayed. This  **Cross-tenant** setting applies to all tenants on this server. To change it, use ARIS Cloud Controller. For further information, refer to **ARIS Cloud Controller (ACC) Command-line Tool** manual.



Prerequisite

- You have the Process Governance administrator (page 110) function privilege.
- The instances have the **Running** status (page 133).

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the relevant process instance under **Processes**.
3. Click  **Increase priority**. The **Prioritized** status is set and displayed in **Details**. The process instance is executed with a higher priority.
4. Click  **Decrease priority** to remove the **Prioritized** status. The **Prioritized** status is removed.
5. To display the process instances with **Prioritized** status, click **Instances**.
6. Click  **Show/Hide filter**. The filter criteria are displayed.
7. Enable () the **Priority status** filter.
8. Click **Apply filter**.

The process instances with **Prioritized** status are displayed.

To prioritize/deprioritize multiple instances simultaneously, open **Instances**, enable the relevant instances () and click  **Increase priority**/ **Decrease priority**. The function is only available if all selected instances meet the prerequisites for prioritization.

14.19 How to handle large volume data

As an alternative to the features in process administration, you can use the reports of ARIS Script to handle large data volumes. For example:

- Delete process instances
- List archived instances
- Delete archived instances
- Unarchive archived instances

We recommend that you do not run these reports during core time, as this can have a significant negative impact on performance.

For detailed information, refer to **ARIS > Help > ARIS Script > Methods for reports and semantic checks > Global objects > Report component interfaces > Process > Process.**

14.20 What is the escalation manager?

The escalation manager is the user who is notified when a human task is not completed by any executor by the due date. It is specified in the data flow diagram or in the model using an organizational element and the **is escalated to** connection.





14.21 Find and correct problems in processes

To ensure a smooth process flow the Process Governance administrator must be able to query information on processes and intervene, if required. Information and functions are provided in process administration (page 103) in ARIS Connect for this purpose. If problems occur during process execution, for example, if an error occurs during an automated task or the recipient of an e-mail message is not recorded as a user, the Process Governance administrator is informed by e-mail.

14.21.1 List processes and display instance/version

You can display a list of process instances in their various statuses (page 133). You can check if process instances failed so that you can correct (page 127) and restart them, if required.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click **Instances**. The list of process instances is displayed.
3. Click  **Filter** to restrict the number of process instances displayed based on various criteria.
4. Select filter criteria.
5. Click **Apply filter**. The list is filtered according to the selected filter criteria. To display the unfiltered list of process instances, click **Reset filter**.
6. To display a specific instance/version, move the mouse pointer over the relevant table row and click  **Display process instance** or  **Display process version**. The instance/version is selected in the Explorer tree.

The list of process instances in their various statuses is displayed.

You can also display instances or versions in the Explorer tree by using **Human tasks**.

ARIS video tutorial


Find and correct problems in processes

(<http://www.ariscommunity.com/videos/learn-how-find-problems-process-and-correct-processes>) (approx. 4 minutes)

14.21.2 Review input and output data of activity

When you receive an e-mail informing you that an activity has failed you can review the input and output data of the activity to find out whether they caused the failure.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Select the process instance of the executable process containing the failed activity. You were informed about the relevant activity in the notification.
3. Click **History**.
4. Click the activity whose execution failed.

Input and output data of the activity are displayed. Review the data.

You can change the output data using the function Skip activity (page 124).

ARIS video tutorial

Find and correct problems in processes

(<http://www.ariscommunity.com/videos/learn-how-find-problems-process-and-correct-processes>) (approx. 4 minutes)



14.21.3 Restart failed activities

You can restart failed activities. You are notified by e-mail if an activity failed.

Prerequisite

Restart failed process instances (com.idsscheer.retry.failed.instances.on.restart) is enabled in the configuration (page 151) ( **Application launcher** >  **Administration** >  **Configuration** > **Process Governance** > **Infrastructure**). By default, this property is disabled.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the process instance of the executable process containing the failed activity. You were informed about the relevant activity in the notification.
3. Click **History**.
4. Move the mouse pointer over the activity whose execution failed. The buttons of the available functions are displayed.
5. Click  **Retry**.

The activity is restarted with the same data as the failed activity.

If the activity cannot be restarted, you will receive a notification. You can skip (page 124) the activity.

ARIS video tutorial



Find and correct problems in processes

(<http://www.ariscommunity.com/videos/learn-how-find-problems-process-and-correct-processes>) (approx. 4 minutes)

14.21.4 Skip failed activities

If a restart (page 123) is impossible, you can skip failed activities. You are notified by e-mail if an activity failed.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the relevant process instance under **Processes**.
3. Click **Activities**. The process instance activities are listed.
4. Move the mouse pointer over the activity you want to skip. The buttons of the available functions are displayed.
5. Click  **Skip activity**. If output data was specified for the activity, a dialog opens for you to correct the data and thus avoid further failure. If no output data was specified for the activity, the activity is skipped immediately.
6. Change the output data.
7. Click **Save**.

The process continues with the next activity.

ARIS video tutorial




Find and correct problems in processes

(<http://www.ariscommunity.com/videos/learn-how-find-problems-process-and-correct-processes>) (approx. 4 minutes)

14.21.5 Skip human tasks

You can skip activities of instances that you suspended before. This is useful if the activity would fail or if none of the executors assigned to the human task are available and therefore the instance could not be completed.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the relevant process instance under **Processes**.
3. Click  **Suspend**. The execution of the process instance is suspended. It has the status **Suspended**.
4. Click **Activities**. The process instance activities are listed.
5. Move the mouse pointer over the human task you want to skip. The buttons of the available functions are displayed.
6. Click  **Skip activity**. If output data was specified for the activity, a dialog opens for you to correct the data and thus avoid further failure. If no output data was specified for the activity, the activity is skipped immediately.
7. Change the output data.
8. Click **Save**.

The human task is skipped and set to **Completed** status. Now you can resume (page 114) the instance. If this human task is the last activity of the process, the instance is also set to **Completed** status and therefore does not need to be resumed.

ARIS video tutorial





Find and correct problems in processes

(<http://www.ariscommunity.com/videos/learn-how-find-problems-process-and-correct-processes>) (approx. 4 minutes)

14.21.6 Correct and restart failed process instances

You can restart failed process instances. You are notified by e-mail if a process instance failed.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click **Instances**. The list of process instances is displayed.
3. Click  **Filter**, select the filter **Status** and the status **FAILED**.
4. Click **Apply filter**. The list of failed process instances is displayed.
Alternatively, you filter process instances with the filter **ID** by entering the ID of the failed process instance, which you received in the notification.
5. Move the mouse pointer over the process instance you want to correct. The buttons of the available functions are displayed.
6. Click  **Display process instance**. The instance is displayed.
7. Click **Console** to obtain further information on why the instance failed.
8. Correct the errors that led to the process instance failing.
9. Click the relevant process instance.
10. Click **History**.
11. Move the mouse pointer over the activity whose execution failed. The buttons of the available functions are displayed.
12. Click  **Retry**.

The activity is restarted and the process instance continues.

ARIS video tutorial

Find and correct problems in processes

(<http://www.ariscommunity.com/videos/learn-how-find-problems-process-and-correct-processes>) (approx. 4 minutes)


14.22 Display information

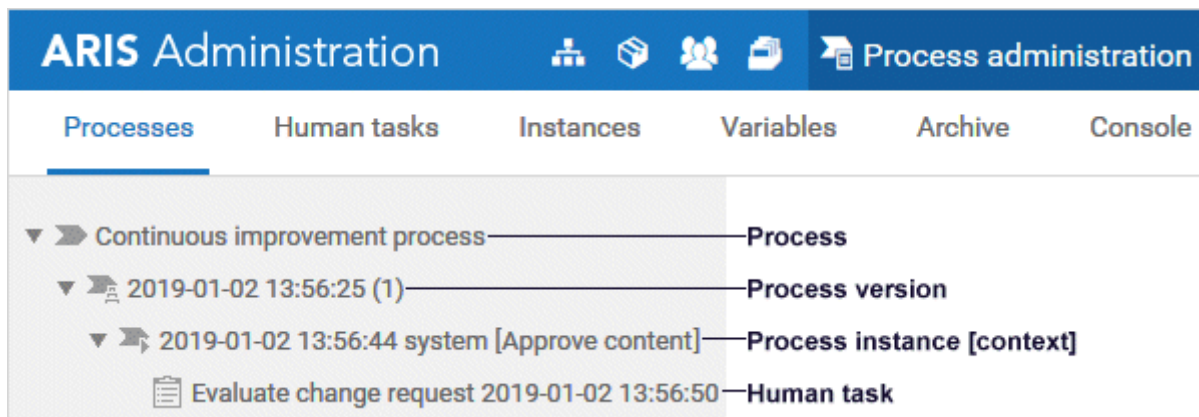
Process administration in ARIS Connect provides functions (page 103) for process automation and information about executable processes.

14.22.1 Display information about executable processes







In process administration, existing executable processes are displayed. You receive detailed information on processes, process versions/instances, and human tasks.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the process, process version, process instance, or human task.



3. Activate the required function in the navigation bar.

The information available for this item is displayed. Processes versions for which a Process Governance Simulation was performed are marked with , simulation runs and process instances with . Processes for which a recurrence has been configured in ARIS Architect are identified in process administration by the symbol . Statistics data in the form of charts (page 137) for Governance processes are available under  **Application launcher** >  **Administration** >  **Charts** > **Governance** > **Processes**.

ARIS video tutorial

Process administration overview


(<http://www.ariscommunity.com/videos/process-administration-aris-connect-overview>)

(approx. 4 minutes)


14.22.2 Display information about activities

You can display details of an activity.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the relevant process instance under **Processes**.
3. Click **History**.
4. Click the relevant activity in the table.
5. Click **Input activities**.
6. Click **Show associated activity in the history** to display the corresponding activity in the history table. Then click **Input activities** again.

Alternatively, you can click **Used by** so that all activities for which the selected activity acts as an input activity are displayed.



7. Click **Input variables** or **Output variables** to show the values read (input) or stored (output) during execution of an activity.
8. Click **Input data** or **Output data** to check the data. Additionally, you can click  **Show details** to display the XML data. For restartable failed activities the tracking ID is displayed.

The relevant details are displayed.

14.22.3 Display human tasks of process instances

You can display the human tasks associated with a process instance.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the process instance whose human tasks you want to display.
3. Click  **Show tasks**.

The associated human tasks are displayed.

ARIS video tutorial

Process administration overview



(<http://www.ariscommunity.com/videos/process-administration-aris-connect-overview>)

(approx. 4 minutes)

14.22.4 Display information about variables

You can display detailed information of a variable (page 109), for example, value, value history, XML data.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click **Variables** to display the variables of all processes. Or click the relevant process version or process instance under **Processes** and then click **Variables**. The variables used with their value, timestamp, type and scope are displayed.
3. To display the XML data of the variable value, click a variable in the table.
4. To show the previous values of a variable including their timestamps, click **History**. Additionally, you can show the values read (input) or stored (output) during execution of an activity.
5. Once you selected a variable in the table, you can use  **Show details** to display or hide **Value as XML** and **History**.

The details of the variable selected are displayed.

To export (page 113) the content, click  **Export as a CSV file** in the navigation bar.



14.22.5 Display and delegate executors of human tasks



You can display the executors of human tasks and delegate tasks.

Prerequisites



- A task must have been selected in the list.
- The task must have been assigned to a user group.
- The status of this task is **New** or **In process**.
- The user to whom the task has been transferred belongs to the allowed group (data flow: **Group of allowed delegates**).

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click **Human tasks**.
3. Move the mouse pointer over the relevant task. The buttons of the available functions are displayed.
4. Click  **Show details**. The human task is displayed in **Processes**.

5. Click  **Navigate to occurrence in Explorer tree**, to show the location of the human task.
6. Click **Assignments**.
7. Move the mouse pointer over the relevant task. The buttons of the available functions are displayed.
8. Click  **Delegate task**. The corresponding dialog opens.
9. Enter the first characters of the group, user name, first name, or last name, and click **Find**. If hits exist for the current search, the results are displayed.
10. To select a group or user, select the relevant element. If you select a group, you also need to select a user.
11. Optionally, enter a comment, such as a reason or notes for the new executor.
12. Click **Delegate**.

The task is passed on to the selected executor and its status (page 134) is displayed as **Delegated**.

Statistics data in the form of charts (page 137) for human tasks are available under  **Application launcher** >  **Administration** > **Charts** > **Governance** > **Human tasks**.

ARIS video tutorial

Process administration overview

(<http://www.ariscommunity.com/videos/process-administration-aris-connect-overview>)

(approx. 4 minutes)

14.22.6 Which status can activities have?

An activity can have any of the following statuses:

- **ACTIVE**
The activity is just being performed.
- **TERMINATED**
The Process Governance administrator terminated the activity manually during process execution. This may be called for if, for example, the executable process is no longer relevant.
- **FAILED**
The activity could not be performed completely due to an error. Failed activities can be restarted after the error is fixed.
- **SUSPENDED**
The activity has been automatically canceled.
- **COMPLETED**
The activity was completely performed.

14.22.7 Which status can process instances have?

A process instance can have any of the following statuses:

- **Running**

The process instance is running the process.

- **Suspended**

The Process Governance administrator suspended (page 114) the process instance manually during process execution. This can be useful, for example, if a server outage would cause the process execution to fail.

- **Terminated**

The Process Governance administrator terminated (page 115) the process instance manually during process execution. This may be called for if, for example, the executable process is no longer relevant.

- **Failed**

The process instance was not able to pass through the process completely due to an error. Failed process instances can be restarted (page 127) after the error is fixed.

- **Idle**

The process instance is in wait state because something unforeseen has happened while the process was passed through. The Process Governance administrator must check and resolve this.

- **Completed**

The process instance has completely passed through the process.

14.22.8 What statuses can tasks have?

Tasks can have the following statuses in **My tasks**:

- **New**

The task has not been edited since it was assigned, or it was reset.
- **In process**

The task was partially edited, and the editor then finished editing by selecting **Save** to save the current input and resume editing at a later time.
- **Active**

Tasks to be edited, that is, tasks in the **New** or **In process** state.
- **Overdue**

The specified processing time of the task has expired. If the list contains overdue tasks, the number is displayed in the top bar.
- **Suspended**

The process instance that triggers this human task has been suspended in the process administration.
- **Being edited by another user**

This status is set automatically as long as a task that was assigned to several possible executors is currently being edited by one of them. Tasks with this status are displayed with a gray background in the list.
- **Failed**

The task could not be performed because a problem occurred.
- **Completed**

Editing of the task was completed with **OK**. Further editing is no longer possible. However, you can open the task with a double-click to view details. Tasks with this status are displayed with a gray background and with strikethrough formatting in the list.
- **Passed on**

Editing of the task was passed on from the executor to another user for a specific period of time.
- **Delegated**



Editing of the task was passed on permanently from the original assignee to another user. The task remains in the list of the original assignee with this status.
- **Task assignment failed**

The task was not completed by any executor before its due date. The group of executors contained either no executors or no active executors.



14.23 Handle simulation

The simulation of executable processes (Process Governance Simulation) enables you to test the modeling of processes before release. The automated execution of all process passes and the possible data combinations is less error-prone and quicker than the manual method.

14.23.1 Display simulation information



In process administration, the processes for which Process Governance Simulation was performed are displayed. Processes versions for which a Process Governance Simulation was performed are marked with , simulation runs and process instances with . You receive further information and tips regarding errors. If the simulation of a process instance fails, the Process Governance administrator receives a notification and a message is displayed in Console (page 106).

Procedure



1. Open (page 103)  **Process administration** in ARIS Connect.
2. Click the relevant process instance under **Processes**.
3. Click **Details** (page 106), if not already activated, to display information about the status and progress of the simulated process instances.
4. To display simulation data for simulated activities, click **History** (page 107), and activate the relevant activity in the table.
5. If you need an overview of the process instances a simulation was performed for, click **Instances** (page 108). The simulated activities are marked with  in the **Simulated** column.
6. To display messages regarding the process instance, activate the Console (page 106) bar. The various process passes of the instance are displayed under the process instance, for example, when an XOR operator is used in the process.

This information can be used to resolve modeling errors and optimize the process.

14.23.2 Release simulated process



You can release process versions that were created and checked by Process Governance Simulation, that is, transform the simulated process into a normal process. It is not possible to start a governance process for processes generated by the simulation (/). This can be done after the transformation into a released process.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Select the relevant process version.
3. Click  **Transform simulated version into a normal process.**

The process version is transformed into a normal process.



14.23.3 Delete simulation runs

You can delete terminated simulation runs to make process administration clearer. Processes versions for which a Process Governance Simulation was performed are marked with , simulation runs and process instances with .

Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Open (page 103)  **Process administration** in ARIS Connect.
2. Under **Processes** click the relevant simulation run.
3. Click  **Delete.**
4. Confirm the confirmation prompt by clicking **OK.**

The simulation run is deleted and removed from Process administration.

15 Use charts



Charts represent accumulated statistics data graphically.

15.1 Display charts

You can view statistics data for the **Users**, **Documents**, **Modeling**, and **Governance** areas as charts. Charts can be used, for example, to perform real-time checks.

Prerequisite


You have one of the following function privileges:

- **User administrator** (charts on user management)
- **Database administrator** (charts on modeling)
- **Document administrator** (charts on ARIS document storage)
- **Process Governance administrator** (charts on Process Governance)
- **Generate user statistics (com.aris.umc.audit.enabled)** is enabled in the configuration (page 244) (**User management > Security > Advanced settings**). If **License monitoring (User management > License monitoring > General)** is enabled, **Generate user statistics** is automatically enabled. Only the **Users > License usage** chart is displayed regardless of this activation.

Procedure

1. Click  **Application launcher** >  **Dashboards**.
2. Click the relevant area (**Users**, **Documents**, **Modeling**, **Governance**).

The charts for the selected area are displayed. The user management charts do not contain any data for technical users by default (system, superuser, arisservice, and guest). Move the mouse pointer over a chart to view an explanation.

You can update the charts to reflect the current state by clicking  **Refresh**. You can also export (page 58) statistics on usage patterns, assignments, changes to data and database items made by the user, the information used most often or the information used last, etc.

15.2 What charts exist?

There are charts from the user management, document storage, modeling, and Process Governance (processes and human task) areas. The user management charts do not contain any data for technical users by default (system, superuser, arisservice, and guest). Move the mouse pointer over a chart to view an explanation.

16 Configure ARIS Connect



Each tenant has its own configuration. Configuration administrator (page 48) can configure and customize each tenant to meet specific requirements.

16.1 Configure the user interface

By default, ARIS Connect provides the classic configuration set and the default configuration set as examples. Using these as basis, you can define modification sets to customize how data is displayed in the portal. You can either specify item types in the modification sets or specify item types in the content type configuration.

It is recommended to save the customized modification set once it is finished. After a software update, you can restore the customized modification set to restore the look and feel of the portal.

16.1.1 Publish databases




Publish the databases you want to make available under **Published content**. There, users with a **Viewer** or **Designer** license can access the fact sheets of the models and objects of the databases.

To start executables and download SAP documents, or to have the ARIS Online Guide available, you must import (page 424) SAP-related configuration sets for the portal and publish the database in **Published content** (page 139, page 427).

Prerequisite

- You have the **Database administrator** function privilege.
- You have the **Publishing administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**.
2. Click **Portal** > **Publish databases** if it is not already selected. The  **Configuration** tab displays the **Publish databases** area. All available databases are displayed.
3. Enable the check boxes of the databases you want to publish in **Published content**.
4. For versioned databases, select the relevant version.
5. Click **Apply**.

The content of the databases is published in **Published content** in the selected configuration or modification set. If databases are available in **Published content** they cannot be deleted in ARIS.

16.1.2 Change sort order of published databases

You can sort published databases that are offered by the process portal.

Prerequisite

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

Procedure

1. Click your initials. The user menu opens.
2. Click **Administration**.
3. Click **Portal > Publish** on the **Configuration** tab. All available databases are displayed. The check boxes of published databases are enabled. If you want to publish further databases to be shown in the process portal, enable the check boxes of these databases. (page 139, page 427)
4. Position the mouse pointer over the row of the database you want to move. The move symbols are displayed.
5. Click ▲ **Move up** to shift the database one row up.
6. Click ▼ **Move down** to shift the database one row down.
7. Click ▬ **Move to top** to shift the database to the top of the database list.
8. Click **Apply**.

You have changed the sort order of the published databases. The published database at the top of the list is the default database (page 141).



16.1.3 Specify a default database

You can specify that versions of models can be compared. This applies to versionable databases that contain at least one version.

Prerequisite

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

Procedure

1. Click your initials. The user menu opens.
2. Click **Administration**. The  **Configuration** tab displays the **Publish databases** area. All available databases are displayed. The check boxes of published databases are enabled. If you want to publish (page 139, page 427) further databases to be shown in the process portal, enable the check boxes of these databases.
3. Move the mouse pointer over the row of the published database you want to define as the default database. The move symbols are displayed.
4. Click  **Move to top** to shift the database to the top of the database list.
5. Click **Apply**.

You have defined the default database.

16.1.4 Allow model comparison

You can allow model comparison of versions of a database or of models between different databases.




IN A DATABASE


You can specify that models can be compared with a version. That is valid for versionable databases that have been published and contain versions.

Prerequisite

- You have the **Publishing administrator** function privilege.
- The database in use is versionable and contains versions.

Procedure

1. Click your initials. The user menu opens.
2. Click **Administration**. The  **Configuration** tab displays the **Publish databases** area. All available databases are displayed. The check boxes of published databases are enabled.
3. Move the mouse pointer over the row of the published database you want to allow model comparison. The  **Allow model comparison** symbol is displayed.
4. Click  **Allow model comparison**. The **Select comparison database** dialog is opened.
5. Leave the **Comparison enabled** check box enabled.
6. Click the **Version** field and select the version to be used for model comparison.
7. Click **Save**.

You have defined with which version models current models of the database can be compared. The  **Allow model comparison** symbol of the database is colored and users can compare the model versions in the fact sheet **Diagram**.




BETWEEN DATABASES


You can specify that models of different databases can be compared. That is valid for versionable databases that contains at least one version.

Prerequisite

- You have the **Publishing administrator** function privilege.
- The database in use is versionable and contains versions.

Procedure

1. Click your initials. The user menu opens.
2. Click **Administration**. The  **Configuration** tab displays the **Publish databases** area. All available databases are displayed. The check boxes of published databases are enabled.
3. Move the mouse pointer over the row of the published database you want to allow model comparison. The  **Allow model comparison** symbol is displayed.
4. Click  **Allow model comparison**. The **Select comparison database** dialog is opened.
5. Click the **Database** field and select the database to be used for model comparison.
6. Click the **Version** field and select the version to be used for model comparison.
7. Click **Save**.

You have defined with which version models of which database current models of the current database can be compared. The  **Allow model comparison** symbol of the database is colored and users can compare the model versions in the fact sheet **Diagram**.

16.2 Configure user management

You can customize general settings of your system's user management.




16.2.1 Import configuration

You can import configurations, which were, for example, exported from a different tenant, into any tenant or installation and use them there. This is an easy way to specify properties that are valid for all tenants on all tenants. This includes, for example, security settings or the configuration of user management systems such as LDAP or SCIM. We recommend that you backup (page 146) your existing configuration before you import a configuration in case that the imported configuration does not meet your expectations.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **User management**.
4. Click  **Import configuration file**.

The **Import configuration file** dialog opens. Navigate to the location where the configuration file is stored and import it. The new configuration is active immediately and no system restart is required.





16.2.2 Export configuration

You can export configurations in order to import them into any tenant or installation and use them there. This is an easy way to specify properties that are valid for all tenants on all tenants. Only changed properties will be exported. However, cross-tenant are not exported. Cross-tenant properties are properties that are used system-wide and can only be changed using ARIS Cloud Controller. For more information, refer to **ARIS Cloud Controller (ACC) Command-line Tool manual**.

Prerequisite

- You have the **Technical configuration administrator** function privilege.
- You have allowed pop-ups for the pages of ARIS Administration.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **User management**.
4. Click  **Export current configuration as a file**.

You can save the configuration file at the relevant location for further use.


16.2.3 Configure user for impersonation





Impersonation enables a user to assume another user account. The user can then perform operations that are actually only permitted for the other account. This configuration must be set for each tenant.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Log in to User Management.
Click the link that was provided to you or that you have saved as a bookmark in your browser, for example, **http://myServer:1080/#myTenant/adminUsers**. The **Log in** dialog opens.
2. Enter the name of the infrastructure tenant in the  **Tenant** field, for example, **master**.
3. Enter your user name and your password.
4. Click the user for which you want to allow impersonation.

5. Click **Privileges**. The list of function privileges is displayed.
6. Click the user for which you want to allow impersonation.
7. Activate the **Impersonation** function privilege.
8. Log out.
9. Log in (page 3) to ARIS Connect.
10. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
11. Click  **Configuration**.
12. Click **User management**.
13. Click the arrow next to **Users**.
14. Click **General**.
15. Click  **Edit**.
16. Click in the **Impersonation target users** field.
17. Enter the users for which you want to allow impersonation as a comma-separated list.

Warning

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

18. Click  **Save**.

You have allowed users to use impersonation.

16.2.4 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, for example, master (page 146). 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, for example, **default**, the user **superuser** must be defined as the target for impersonation (page 429). Impersonation enables users to back up tenants in which they do not exist as a user.

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

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

16.2.5 What is the default user group?

You can configure (page 261) a default user group in the ARIS Administration. This group must exist in the ARIS Administration. A user is automatically assigned to this default user group whenever a user is created.

All local users who were created after specifying a default user group are automatically assigned to this group.

You can specify an LDAP user group as default user group. All LDAP users in the LDAP group are assigned to this group.

Hidden users such as, for example, arisservice, are never assigned to the default user group.

16.2.6 Customize infrastructure





You can customize general settings of your system infrastructure, for example, format of e-mail in HTML.


You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.


Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click **Infrastructure**. To configure further settings, click a configuration category (page 151).
5. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

6. Adjust your settings.
7. Click  **Save**.

You have customized your system configuration.

16.2.7 Infrastructure properties

You can customize your system infrastructure (page 150) as required.

You can change properties that are highlighted as cross-tenant properties only by using the ARIS Cloud Controller command-line tool. To change the settings, enter the following:

```
reconfigure umcadmin_<size of your installation, s, m, or l> JAVA-D<property name>="<value>"
```

Example

```
reconfigure umcadmin_m JAVA-Dcom.aris.umc.loadbalancer.url="https://myserver.com"
```

Key	Description
com.aris.umc.version	<p>Build number</p> <p>Build number of ARIS Administration. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>10.0.4-SNAPSHOT</p>
com.aris.umc.loadbalancer.url	<p>Load balancer URL</p> <p>Specifies the URL of the load balancer. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p>

Key	Description
com.aris.umc.notification.useHttpLinks	E-mails with HTTP URLs only Specifies whether or not the HTTP protocol is used instead of the HTTPS protocol in e-mails. Valid input true, false

HTTP CLIENT

Key	Description
com.aris.umc.client.connect.timeout	Connection timeout (in milliseconds) Specifies the duration after which a client's connection attempt is canceled. This is defined in milliseconds. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual . Valid input Integer > 0
com.aris.umc.client.idle.timeout	Idle timeout (in milliseconds) Specifies the wait time timeout of the ARIS Administration REST client. This is defined in milliseconds. Valid input Integer > 0

Key	Description
com.aris.umc.client.read.timeout	Read timeout (in milliseconds) Specifies the wait time timeout of the REST client for read access. This is defined in milliseconds. Valid input Integer > 0
com.aris.umc.client.connections.max	Maximum connections (total) Specifies the maximum number of connections that may be established simultaneously. If additional connections are to be established, they are refused. Valid input Integer > 0
com.aris.umc.client.connections.perhost	Maximum connections (per host) Specifies the maximum number of connections that may be established simultaneously per host. If additional connections are to be established, they are refused. Valid input Integer > 0
com.aris.umc.client.retry.max	Number of retries Specifies the maximum number of retries. Valid input Integer > 0

Key	Description
com.aris.umc.ssl.host.verification.active	<p>Host name verification</p> <p>Specifies whether the verification of the SSL host name is activated. Verification is enabled by default.</p> <p>Valid input</p> <p>true, false</p>

ADVANCED SETTINGS

Key	Description
com.aris.umc.remote.clients	<p>Allowed remote clients</p> <p>Comma-separated list of client IPs that uses the remote interface of ARIS Administration.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.config.cache.ttl	<p>Configuration cache lifetime</p> <p>Specifies the lifetime of the configuration cache in seconds. The configuration is reloaded after the time set here. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p>

Key	Description
com.aris.umc.config.encrypted	<p>Encrypted properties</p> <p>Specifies a comma-separated list of encrypted property keys.</p> <p>Valid input</p> <p>List of strings</p> <p>Example</p> <p>com.softwareag.aris.umc.ldap.service.pwd</p>
com.aris.umc.jaas.login.context	<p>JAAS login context</p> <p>Specifies the login name for the JAAS context. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>UMC-DB</p>
com.aris.umc.basicauth.tenant	<p>Default tenant</p> <p>Specifies that the default tenant is used for authentication. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>String</p>

Key	Description
com.aris.umc.infrastructure.tenant	<p>Infrastructure tenant</p> <p>Specifies the tenant with special privileges for managing other tenants, components, and the configuration in ARIS Administration.</p> <p>By default, the master tenant is the infrastructure tenant. The system users system and superuser have administrative privileges, that is, they can access ARIS Administration and Tenant Management.</p> <p>Users with the relevant privileges can specify other infrastructure tenants in ARIS Administration.</p> <p>Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p>

16.2.8 Kerberos

Kerberos is a computer network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.





16.2.8.1 Customize Kerberos settings


You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration. Adapt your Kerberos settings.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **Kerberos**.
5. Click a configuration category (page 159).
6. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

7. Adjust your settings.
8. Click  **Save**.

You have customized your system configuration.







16.2.8.2 Upload Kerberos configuration files

You can upload the Kerberos configuration file or the key table.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **Kerberos**. The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.
5. Activate the **General** configuration category.
6. To upload the key table file, click  **Upload** under the **Key table** field. To upload the configuration file, click  **Upload** under the **Configuration file** field. You find this file on your installation medium under **Add-ons\Kerberos**. The dialog for uploading a file opens.
7. Select the relevant file.

You have uploaded a configuration file.

CREATING A KEY TABLE FILE

If you have no key table file available, generate a key table file using the JRE tool **ktab.exe**. To do so, enter the following in the console:

```
ktab -a userPrincipalName@REALM password -n 0 -append -k umc.keytab
```

DISPLAY EXISTING KEY TABLE FILE

You can display the content of an existing key table file using the JRE tool **ktab.exe**. To do so, enter the following in the console:

```
ktab -l -e -t -k FILE:C:\<file location of the umc.ktab file>\umc.ktab
```


16.2.8.3 Kerberos properties

You can configure Kerberos (page 157) as required.

You can change properties that are highlighted as cross-tenant properties only by using the ARIS Cloud Controller command-line tool. To change the settings, enter the following:

```
reconfigure umcadmin_<size of your installation, s, m, or l> JAVA-D<property name>="<value>"
```

Example

```
reconfigure umcadmin_m JAVA-Dcom.aris.umc.loadbalancer.url="https://myserver.com"
```

GENERAL

Key	Description
com.aris.umc.kerberos.active	Use Kerberos Specifies whether a Kerberos-based login is allowed. Valid input true, false

Key	Description
com.aris.umc.kerberos.kdc	<p>KDC</p> <p>Specifies the fully qualified name of the central Key Distribution Center (KDC). This is usually the fully qualified host name of the LDAP server.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>mykdc.mydomain.com</p>
com.aris.umc.kerberos.realm	<p>Realm</p> <p>Specifies the realm of Kerberos tickets. Fully qualified domain name in uppercase letters.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>MY.CORP.SOFTWAREAG.COM</p>

Key	Description
com.aris.umc.kerberos.servicePrincipalName	<p>Principal</p> <p>Specifies the name of the technical user used for verifying Kerberos tickets.</p> <p>If Kerberos is used, each user, computer or service provided by a server must be defined as a principal.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>MyLogin</p>
com.aris.umc.kerberos.keyTab	<p>Key table</p> <p>Specifies the location of the keytab file that is used for Kerberos tickets.</p> <p>The file can be uploaded directly.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>C:/safePlace/krb-umc.keytab</p>

Key	Description
com.aris.umc.kerberos.config	<p>Configuration file</p> <p>Storage location of the configuration file for Kerberos.</p> <p>The file can be uploaded directly.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>./config/Kerberos/krb5.conf</p>

ADVANCED SETTINGS

Key	Description
com.aris.umc.kerberos.debug	<p>Debug output</p> <p>Specifies whether debug output is allowed for Kerberos operations.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.kerberos.allowLocal Users	<p>Allow local users</p> <p>Specifies whether the LDAP connection is mandatory for Kerberos-based login. If this option is enabled, Kerberos is used for the login of local users also.</p> <p>Valid input</p> <p>true, false</p>

Key	Description
com.aris.umc.kerberos.validateuser	<p>Ignore realm from service ticket</p> <p>Specifies whether or not the realm defined for the user principal name provided in the Kerberos ticket is to be ignored. The default value is false.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.kerberos.tenant.	<p>Default tenant</p> <p>Specifies the default tenant for a Kerberos-based login. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>true, false</p>

16.2.9 LDAP

LDAP is an application protocol from the network technology. LDAP enables information from a distributed, location-independent, and hierarchical database in a network to be queried and modified.

16.2.9.1 Add LDAP server

LDAP enables information from a distributed, location-independent and hierarchical database in a network to be queried and modified.







You can use multiple LDAP servers with ARIS.

The migration to multiple LDAP servers is irreversible. Any existing LDAP data needs to be deleted manually before the migration.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **LDAP**.
5. Click **General settings**.
6. Click  **Edit**.
7. Enable **Use LDAP**.
8. Optional: Enable **Activate multiple LDAP integration** and confirm the **Property value change confirmation** dialog with **OK**.
9. Click  **Save**.
10. Click  **Add**. The **Add LDAP server** dialog opens.
11. Enter the following (page 179):
 - ID of the LDAP server
 - Display name of the LDAP server
 - LDAP server URL
 - LDAP server fallback URL

- User name of the user who has access to the LDAP content
- Password of this user
- Specify whether or not SSL should be used and in which mode
- Specify whether or not host names and certificates should be verified
- Specify the connection timeout
- Specify the read timeout

12. Click **Save**.

13. Click  **Save**.

You have added an LDAP server.

If you want to specify more than one LDAP server, proceed with step 10 of the procedure steps mentioned above.

16.2.9.2 Test connection to an LDAP server





LDAP enables information from a distributed, location-independent and hierarchical database in a network to be queried and modified.

You can use multiple LDAP servers with ARIS.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **LDAP**.
5. Click the arrow next to the relevant LDAP server.
6. Click **Connection**.
7. Click  **Test connection**.

A message is displayed, whether or not the connection to the LDAP server specified is valid.

16.2.9.3 Edit connection to an LDAP server






LDAP enables information from a distributed, location-independent and hierarchical database in a network to be queried and modified.

You can use multiple LDAP servers with ARIS.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **LDAP**.
5. Click the arrow next to the relevant LDAP server.
6. Click **Connection**.
7. Click  **Edit**.
8. Enter the following (page 179):
 - ID of the LDAP server
 - Display name of the LDAP server
 - LDAP server URL
 - LDAP server fallback URL
 - User name of the user who has access to the LDAP content
 - Password of this user
 - Specify whether or not SSL should be used and in which mode
 - Specify whether or not host names and certificates should be verified
 - Specify the connection timeout
 - Specify the read timeout
9. Click  **Save**.

You have edited an LDAP server connection.





16.2.9.4 Upload LDAP truststore file

You can upload the truststore file.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **LDAP**.
5. Click **General settings**.
6. Click **Truststore**. You must have generated a truststore file.
7. Click  **Upload**. The **Truststore** dialog opens. Select the truststore file you want to use.
8. Select the relevant file.

You have uploaded a truststore file

16.2.9.5 Customize LDAP settings




LDAP enables information from a distributed, location-independent and hierarchical database in a network to be queried and modified.


You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.


Prerequisite


You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **LDAP**.
5. Click a configuration category (page 179).
6. Click the arrow next to the relevant LDAP server.

7. Click a configuration category (page 179).
8. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

9. Adjust your settings.
10. Click  **Save**.

You have customized your system configuration.






16.2.9.6 Customize ARIS for LDAP server operations

You can configure ARIS for LDAP server operations.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **User management**.
4. Click the arrow next to **LDAP**.
5. Click **General settings**.
6. Click  **Edit**.
7. Enable **Use LDAP**.
8. If you want to upload a configuration, ensure that you have disabled pop-up blockers in the browser.
Click **Truststore**. You must have generated a truststore file.
9. Click  **Upload**. The **Truststore** dialog opens. Select the truststore file you want to use.
10. Click the arrow next to the relevant LDAP server.
11. Configure the URL for the LDAP system. Click **Connection**.
12. Enter an ID, a name, and the URL in the **Server URL** field, for example:
`ldap://hgcc.mycompany.com:3168`.
13. Configure the path to the backup system in the **Server URL (fallback)** field. This backup system takes over automatically if the LDAP server cannot be reached via its primary URL.
14. Click **Behavior**.

15. Enter the Path to the user group in the **Group search paths** field.
16. Enter the Path to the users in the **User search paths** field.

To enable the function of following referrals of users to other directories, enter **follow** in the **Referral** field.

To disable the above behavior, enter **ignore** in the **Referral** field.

If you leave this entry blank, referrals are not followed.

Optional: To ensure that the import of LDAP users is carried out despite any errors that might occur, for example, if names are redundant, click **Global settings > Advanced settings** and enable **Skip errors**.

Please note that system performance is significantly deteriorated if you enable this option.

You have configured ARIS for LDAP server operations.

16.2.9.6.1 Configure secure communication

You can encrypt the communication between ARIS and the LDAP server.

To do so, you have two mutually exclusive options:

- **STARTTLS**

This transforms a connection that was originally untrusted into an encrypted connection without using a specific port.

- **SSL**

The connection between ARIS and the LDAP server is established using a specific port.

Prerequisite

- The LDAP server has a valid SSL certificate and LDAPS is activated.
- ARIS Administration trusts the LDAP server (the SSL certificate of the LDAP server or the certification authority is stored in the JRE database of trustworthy certificates).

STARTTLS

You can use STARTTLS to configure encrypted communication between ARIS and the LDAP server.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.

2. Click  **Configuration**.

3. Click **User management**.

4. Click the arrow next to **LDAP**.

5. Click the arrow next to the relevant LDAP server.

6. Click **Connection**.

7. Click  **Edit**.

8. Configure the URL for the LDAP system. To do so, enter the URL as in the **Server URL** field, for example:

```
ldap://hgcc.mycompany.com:3168.
```

9. Configure the path to the backup system in the **Server URL (fallback)** field. This backup system takes over automatically if the LDAP server cannot be reached via its primary URL.





10. Enable **Use SSL**.

11. Select **STARTTLS** from the **SSL mode** list.

12. ARIS must trust the LDAP server used. Therefore, we recommend that you use the LDAP server with a certificate signed by a public certification authority. If your certificate is signed by a public certification authority and stored in the list of trustworthy certificates of your JRE, you do not need to configure anything else.
13. Upload LDAP truststore file (page 166).

SSL

Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**.
3. Click  **Configuration**.
4. Click **User management**.
5. Click the arrow next to **LDAP**.
6. Click the arrow next to the relevant LDAP server.
7. Click **Connection**.
8. Click  **Edit**.
9. Configure the URL for the LDAP system. To do so, enter the URL as in the **Server URL** field, for example:
`ldap://hqqc.mycompany.com:3168`
10. Configure the path to the backup system in the **Server URL (fallback)** field. This backup system takes over automatically if the LDAP server cannot be reached via its primary URL.
11. Enable **Use SSL**.
12. Select **SSL** from the **SSL mode** list.
13. ARIS must trust the LDAP server used. Therefore, we recommend that you use the LDAP server with a certificate signed by a public certification authority. If your certificate is signed by a public certification authority and stored in the list of trustworthy certificates of your JRE, you do not need to configure anything else.
14. Upload LDAP truststore file (page 166)




16.2.9.6.2 Allow login for LDAP users only

To allow only LDAP users to log in to ARIS Architect and <connect>, you need to configure the system accordingly.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **User management**.
4. Click the arrow next to **LDAP**.
5. Click the arrow next to **General settings**.
6. Click **Advanced settings**.
7. Enable **Prevent login of manually created users**.

Only LDAP users and the following users can log in: **system**, **superuser**, **arisservice**, and **guest**.

16.2.9.6.3 Configure single sign-on (LDAP)

If you are using Microsoft® Active Directory Domain Services, you can configure SSO (single sign-on). This allows users to work with all ARIS components as soon as they are logged in to the domain. Separate login to ARIS components is not required.

Please contact your LDAP administrator before you change any configuration.

Prerequisite

Server

- Users who want to use SSO must have a valid Microsoft® Active Directory Domain Services user login.
- This user is available in ARIS Administration.
- ARIS Administration authenticates against LDAP.
- Microsoft® Active Directory Domain Services supports Kerberos-based authentication (default) and the service principal name of the ARIS Server is entered in the following format: **HTTP/<hostname>**, for example, **HTTP/mypc01.my.domain.com**.




Client

- The client computers and servers are connected to the same Microsoft® Active Directory Domain Services.
- The browser has been configured accordingly.

16.2.9.6.3.1 Use Kerberos



Kerberos is a network authentication, allowing nodes to communicate using an invisible network and to securely make their identity known to each other. Kerberos is the recommended method for user authentication in Microsoft® Windows networks. In addition, it is widely used with Linux operating systems and is designed for use with all major platforms.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **User management**.
4. Click the arrow next to **Kerberos**.
5. Activate the **General** configuration category.

If you do not have a Kerberos configuration file, take the **kbr5.conf** from your installation media under **Add-ons\Kerberos**. Name it, for example, **krb5.conf**, add the following lines, and adjust the configuration to meet your requirements.

```
[libdefaults]
default_tgs_etypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1 aes128-cts
aes128-cts-hmac-sha1-96 aes256-cts aes256-cts-hmac-sha1-96 rc4-hmac
arcfour-hmac arcfour-hmac-md5
default_tkt_etypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1 aes128-cts
aes128-cts-hmac-sha1-96 aes256-cts aes256-cts-hmac-sha1-96 rc4-hmac
arcfour-hmac arcfour-hmac-md5
permitted_etypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1 aes128-cts
aes128-cts-hmac-sha1-96 aes256-cts aes256-cts-hmac-sha1-96 rc4-hmac
arcfour-hmac arcfour-hmac-md5
```

6. To upload the configuration file, click  **Upload** under the **Configuration file** field. You find this file on your installation medium under **Add-ons\Kerberos**.
7. Click  **Edit**.
8. Enable **Use Kerberos**.
9. In the **Principal** field, enter the technical user name given by the administrator.
If the Service Principal Name in the keytab is, for example, **mypc01@MY.DOMAIN.COM**, the values of the property **com.company.aris.umc.kerberos.servicePrincipalName** must contain the Service Principal Name exactly as specified in the keytab file.
10. In the **Realm** field, configure the realm for the Kerberos service. Enter the fully qualified domain name in uppercase letters.
Example: **MYDOMAIN.COM**.
11. In the **KDC** field, configure the fully qualified name of the KDC to be used.

12. Optional:

- a. Click **Advanced settings**.
- b. Enable **Debug output**.

The debug output of the program that the user wishes to log into is saved in the file **system.out** of the respective program. For user management, for example, this is located in the directory **<ARIS installation directory>/work_umcadmin_m/base/logs**.

You have configured SSO using Kerberos in ARIS Administration.

You can use Kerberos with multiple LDAP systems (page 200).

CLIENT CONFIGURATION

Configure the browser settings to allow SSO. SSO has been tested with the following browsers:

- Microsoft® Internet Explorer® (version 11 or higher)
- Mozilla Firefox®

Prerequisite

- You have the **Technical configuration administrator** function privilege.
- SSO must be configured for the servers.
- The browser used supports a Kerberos-based authentication.

You need to empty the Kerberos ticket cache of each client first, in order to avoid obsolete tickets if Microsoft® Active Directory Domain Services were changed. Delete the Kerberos ticket cache by executing the command **klist.exe purge**. If the purge program is not available on the client computer, you can also simply log off the client computer from the domain and log in again.

MICROSOFT® INTERNET EXPLORER®

Microsoft® Internet Explorer® supports Kerberos authentication only if the ARIS Server is part of your local intranet.

Procedure

1. Start Microsoft® Internet Explorer®.
2. Click **Tools > Internet Options**.
3. Activate the **Security** tab and click **Local Intranet**.
4. Click **Sites**, and select **Advanced**.
5. Add the URL of the ARIS Server that was configured for SSO. Add the DNS host name and the IP address of the ARIS Server.

6. Optional: Disable the **Require server verification (https:) for all sites in this zone** check box.
7. Click **Close**, and select **OK**.
8. Click **Custom level** and make sure that no user-defined settings affect your new settings.
9. Find the **User Authentication** section. Verify whether the **Automatic logon only in Intranet zone** option is enabled.
10. Click **OK**.
11. Close and restart Microsoft® Internet Explorer®.

MOZILLA FIREFOX®

In Mozilla Firefox®, you can define trustworthy sites using the computer name, IP address, or a combination of both. You can use wildcards.

Procedure

1. Start Mozilla Firefox®.
2. Enter **about:config** in the address box and press **Enter**. Confirm a message, if required.
3. Enter **network.negotiate** in the **Search** box and press **Enter**, if required.
4. Double-click **network.negotiate-auth.trusted-uris**.
5. Enter the computer name or the IP address of the ARIS Server that you configured for SSO, and click **OK**.
6. Close and restart Mozilla Firefox®.

If you prefer to use an encryption stronger than AES 128bit and this is allowed in your country, replace the JCE Policy file of the JDK of your ARIS Server with the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 (<http://www.oracle.com/technetwork/java/javase/downloads/index.html>). This allows unlimited key length.

If you cannot replace the Policy files, but still want to use SSO, you need to apply a procedure allowed by the JDK for encrypting Kerberos tickets, for example, AES 128bit.





16.2.9.6.3.2 Use SAML

SAML (**S**ecurity **A**ssertion **M**arkup **L**anguage) is an XML framework for exchanging authentication and authorization information. SAML provides functions to describe and transfer security-related information.

Prerequisite

- The SAML identity provider supports the HTTP POST binding as specified by the SAML 2.0 specification.
- You have the **Technical configuration administrator** function privilege.
- If you use multiple LDAP systems, the user names must be unambiguous through all LDAP systems. Otherwise no SSO is possible.
- SSO must be configured for the servers.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **User management**.
4. Click the arrow next to **SAML**.
5. Click **General**.
6. Click  **Edit**.
7. Enable **Use SAML**.
8. Enter the ID of the identity provider in the **Identity provider ID** field.
9. Enter the ID of the service provider in the **Service provider ID** field.
10. Enter the end point of the identity provider that is used for single sign-on in the **Single sign-on URL** field.
11. Enter the end point of the identity provider that is used for single log-out in in the **Single logout URL** field.

You have configured SSO using SAML in ARIS Administration. If you use multiple LDAP systems (page 200), the user names must be unambiguous through all LDAP systems. Otherwise no SSO is possible.

You can use SAML with multiple LDAP systems (page 200).





16.2.9.7 Delete LDAP server

LDAP enables information from a distributed, location-independent and hierarchical database in a network to be queried and modified.

Prerequisite

- You have the **Technical configuration administrator** function privilege.
- Your system is configured to allow multiple LDAP servers.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **LDAP**.
5. Click the arrow next to the relevant LDAP server.
6. Click **Connection**.
7. Click  **Delete**.

You have deleted an LDAP server.

16.2.9.8 LDAP properties

You can customize LDAP (page 167) as required.

GENERAL SETTINGS

Key	Description
com.aris.umc.ldap.active	Use LDAP Specifies whether or not the LDAP integration is enabled. Valid input true, false
com.aris.umc.ldap.multi.active	Activate multiple LDAP integration Specifies whether or not integration of multiple LDAP servers is to be activated. The default value is false . Valid input true, false

Key	Description
com.aris.umc.ldap.connection.count	Number of configured LDAP servers Displays the number of LDAP servers allowed. Valid input Integer Example 2

TRUSTSTORE

Key	Description
com.aris.umc.ldap.ssl.truststore.location	Truststore Specifies where to look for the truststore. Valid input String
com.aris.umc.ldap.ssl.truststore.password	Password Specifies the truststore password. Valid input String

Key	Description
com.aris.umc.ldap.ssl.truststore.type	<p>Type</p> <p>Specifies the truststore type to be used.</p> <p>Valid input</p> <p>String</p>

ADVANCED SETTINGS

Key	Description
com.aris.umc.ldap.debug	<p>Debug output</p> <p>Specifies whether or not debug information for LDAP operations are output.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.ldap.group.import.parent.enabled	<p>Import superior group</p> <p>Specifies whether the superior group is to be imported automatically when the group is imported.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

Key	Description
com.aris.umc.ldap.user.importOnLogin	<p>Import user at login</p> <p>Specifies whether an LDAP user is to be imported automatically during the login attempt.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.ldap.sync.user.importGroups	<p>Import user groups when synchronizing</p> <p>Specifies whether additional user groups are to be imported during user synchronization.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.ldap.attribute.memberOf.resolveOnFirstLogin	<p>Update group associations at login</p> <p>Specifies whether the memberOf attribute is read (true) or not (false). If the value of the property is true, the memberOf attribute is read and the referenced groups are automatically imported. The import of the groups occurs when a user from the group logs in for the first time.</p> <p>Valid input</p> <p>true, false</p>

Key	Description
com.aris.umc.ldap.attributes.paging.enabled	<p>Use attribute value pagination</p> <p>Specifies whether a page break is to be inserted if the server-side limit for valid values is exceeded for attributes, for example, if more than 1,500 attribute values exist.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.ldap.auth.only	<p>Prevent login of manually created users</p> <p>Specifies that only LDAP users may log in. This does not apply to the arisservice, guest, superuser, and system users.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.ldap.entity.cache.size	<p>Cache size</p> <p>Specifies the maximum number of LDAP entities that are cached during an import.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>3500</p>

Key	Description
com.aris.umc.ldap.connection.concurrent.timeout	<p>Pool wait time (in milliseconds)</p> <p>Specifies the maximum amount of time in milliseconds that a connection request may take if the maximum number of connections to the LDAP server was exceeded.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.umc.ldap.connection.pool.size	<p>Pool size</p> <p>Specifies the maximum number of connections that are ready for reuse in a pool. The connection that was used last is discarded when the pool is full.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.umc.ldap.connection.pool.timeout	<p>Pool time (in milliseconds)</p> <p>Specifies the maximum amount of time that a connection remains in a pool. The connection is removed from the pool at the latest after this period of time. This is defined in milliseconds.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.umc.ldap.sync.skipOnFault	<p>Skip errors</p> <p>Specifies whether the LDAP import ignores users or user groups for which errors occurred without showing an error message.</p> <p>Valid input</p> <p>True (without message), False (with error message)</p>

Key	Description
com.aris.umc.ldap.sync.members. searchBottomUp	<p>Use bottom-up method</p> <p>Specifies whether the bottom-up method (memberOf attribute) or the top-down method (hasMember attribute) is applied when associating users to user groups.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.ldap.sync.useDnAs Guid	<p>Use DN as GUID</p> <p>Specifies that the fully qualified name (distinguished name) is used as GUID.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

INDIVIDUAL LDAP SERVER

You can specify the properties of each individual LDAP server.

CONNECTION

Key	Description
com.aris.umc.ldap.connection.id plus the ID defined.	ID Specifies the unique ID of this specific LDAP connection. Valid input String
com.aris.umc.ldap.connection.name plus the ID defined.	Name Specifies the name of this specific LDAP connection. Valid input String
com.aris.umc.ldap.url	Server URL Specifies the URL of the LDAP server. Valid input String
com.aris.umc.ldap.backup.url	Server URL (fallback) Specifies the fallback URL of the LDAP server. This URL is only used if the server cannot be reached via its primary URL. Valid input String

Key	Description
com.aris.umc.ldap.service.user	<p>User name</p> <p>Specifies the user name of the LDAP user.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>arisldapservice</p>
com.aris.umc.ldap.service.pwd	<p>Password</p> <p>Specifies the password of the LDAP user.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.ldap.ssl	<p>Use SSL</p> <p>Specifies if SSL is to be used.</p> <p>Valid input</p> <p>true, false</p>

Key	Description
com.aris.umc.ldap.ssl.mode	SSL mode Specifies the SSL mode (page 170). Valid input String Example STARTTTLS
com.aris.umc.ldap.ssl.host.verification.active	Verify host names Specifies if an SSL host is to be verified. Valid input true, false
com.aris.umc.ldap.ssl.certificate.verification.active	Verify certificates Specifies whether an SSL certificate is to be verified. Valid input true, false
com.aris.umc.ldap.connection.concurrent	Simultaneous connections Specifies the maximum number of simultaneous connections to the same LDAP server. If additional connections are to be established, they are refused. Valid input Integer > 0

Key	Description
com.aris.umc.ldap.timeout	Connection timeout (in milliseconds) Specifies the duration after which the attempt to connect to the LDAP server is canceled. This is defined in milliseconds. Valid input Integer > 0
com.aris.umc.ldap.read.timeout	Read timeout (in milliseconds) Specifies the maximum amount of time that read access may take. This is defined in milliseconds. Valid input Integer > 0

ATTRIBUTE MAPPINGS

Key	Description
com.aris.umc.ldap.attribute.objectclass	objectClass Specifies the attribute that contains the object class. Valid input String Example objectClass

Key	Description
com.aris.umc.ldap.attribute.distinguishedname	<p>DN</p> <p>Specifies the fully qualified name (distinguished name).</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>distinguishedName</p>
com.aris.umc.ldap.attribute.guid	<p>GUID</p> <p>Specifies the LDAP GUID.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Object GUID</p>

GROUP ATTRIBUTE MAPPINGS

Key	Description	Valid input	Example
com.aris.umc.ldap.attribute.group.name	Name Specifies the group name. Valid input String Example Group name	String	Group name
com.aris.umc.ldap.attribute.hasmember	hasMember Specifies the attribute that references the members of a group. Valid input String Example hasMember	String	hasMember

Key	Description	Valid input	Example
com.aris.umc.ldap.group.attribute.s.userdefined	<p>User-defined</p> <p>Specifies a comma-separated list of LDAP attributes that are to be imported as user-defined attributes of a user group.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Description, operating system</p>	String	Description, operating system

USER ATTRIBUTE MAPPINGS

Key	Description	Valid input	Example
com.aris.umc.ldap.attribute.user.name	<p>Name</p> <p>Specifies the user name of a user.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Fragment</p>	String	Fragment

Key	Description	Valid input	Example
com.aris.umc.ldap.attribute.user.firstname	First name Specifies the first name of a user. Valid input String Example John	String	John
com.aris.umc.ldap.attribute.user.lastname	Last name Specifies the last name of a user. Valid input String Example Smith	String	Smith
com.aris.umc.ldap.attribute.user.email	E-mail address Specifies the e-mail address of a user. Valid input String Example john.smith@softwareag.com	String	john.smith@softwareag.com

Key	Description	Valid input	Example
com.aris.umc.ldap.attribute.user.phone	Telephone number Specifies the telephone number of a user. Valid input String Example +491234567	String	+491234567
com.aris.umc.ldap.attribute.user.picture	Picture Specifies the picture of a user. Valid input Location of an image	Location of an image	
com.aris.umc.ldap.attribute.memberof	Member of Specifies the attribute that references the groups of a user. Valid input String Example memberOf	String	memberOf

Key	Description	Valid input	Example
com.aris.umc.ldap.user.attributes.userdefined	<p>User-defined</p> <p>Specifies a comma-separated list of LDAP attributes that are to be imported as user-defined attributes of a user.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Description, operating system</p>	String	Description, operating system

BEHAVIOR

Key	Description
com.aris.umc.ldap.group.objectclass	<p>Group object class</p> <p>Object class of the LDAP groups.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Group</p>

Key	Description
com.aris.umc.ldap.user.objectclasses	<p>User object class</p> <p>Specifies the object class of the LDAP user.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Organizational unit</p>
com.aris.umc.ldap.searchpath	<p>Search paths</p> <p>Specifies a semicolon-separated list of all LDAP search paths.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>OU\=stadt\,OU\=location\, OU\=employees\,DC\=my\,DC\=corp\, DC\=company\,DC\=com</p>

Key	Description
com.aris.umc.ldap.group.searchpath	<p>Group search paths</p> <p>Specifies a semicolon-separated list of all LDAP search paths for user groups. Overwrites the list of general search paths.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>OU\distribution lists\,DC=my,DC=corp\,DC=company\,DC=com</p>
com.aris.umc.ldap.user.searchpath	<p>User search paths</p> <p>Specifies a semicolon-separated list of LDAP search paths for users. Overwrites the list of general search paths.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>OU=employees\,DC=my\,DC=corp\, DC=company\,DC=com</p>

Key	Description
com.aris.umc.ldap.filter.group	<p>Group search filter</p> <p>Specifies the query filter for LDAP groups.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>(&(objectClass=role)(name=y*))</p>
com.aris.umc.ldap.filter.user	<p>User search filter</p> <p>Specifies the query filter for LDAP users.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>(&(sAMAccountName=*))</p>
com.aris.umc.ldap.recursion.depth	<p>Recursion depth</p> <p>Specifies the recursion depth that is to be used for nested groups and users.</p> <p>Valid input</p> <p>1 means one level, 0 means all</p> <p>Example</p> <p>1</p>

Key	Description
com.aris.umc.ldap.pagesize	<p>Page size</p> <p>Specifies the maximum number of entries that are loaded in a single LDAP query.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.umc.ldap.referral	<p>Referrals</p> <p>Defines how referrals to other LDAP systems are processed.</p> <p>Valid input</p> <p>follow means that the referral is automatically</p> <p>Example</p> <p>ignore</p>

16.2.9.9 Using multiple LDAP servers

KERBEROS

Even if you have configured multiple LDAP systems, you can use only one LDAP server with Kerberos authentication.

When using multiple LDAP systems, the **Ignore realm from service ticket** property under **Kerberos -> Advanced Settings** must be enabled.

SAML

If a user is created during login using SAML, the user name will not have any prefix and is assigned to the default user group. This user is not mapped to any LDAP server.

SINGLE SIGN-ON

If users have the same login ID in different LDAP servers, the Single sign-on (page 172) login fails. Users must enter their passwords manually instead.

16.2.10 User defined notifications

You can specify whether or not users are informed about, for example, their creation, password changes, or a license expiration.

16.2.10.1 Customize user-defined notifications

You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.



Variables (page 217) may be used to personalize the content of a notification of ARIS Administration. Variables can be used in both notification subject and body.

Prerequisite

- You have the **Technical configuration administrator** function privilege.
- You have uploaded (page 201) the relevant templates for user-defined notifications.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.

3. Activate **User Management**.
4. Click the arrow next to **User-defined notifications**.
5. Click a configuration category (page 204).
6. Click  **Edit**.
7. Adjust your settings.
8. Click  **Save**.

You have customized your system configuration.





16.2.10.2 Upload templates for notifications

You can upload the templates for user-defined notifications.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **User-defined notifications**.
5. Click a category.
6. Click  **Upload**. The dialog for uploading a file opens.
7. Click **Select file**. Select the relevant file.
8. Click **Upload**. A confirmation prompt is displayed.
9. Click **Close**.

You have uploaded a template for notifications.





16.2.10.3 Customize default HTML templates for notifications

You can customize the templates for user-defined notifications. Variables (page 217) may be used to personalize the content of a notification of ARIS Administration. Variables can be used in both notification subject and body.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **User-defined notifications**.
5. Click a category.
6. Click  **Upload**. The corresponding dialog opens.
7. Enable **Advanced template configuration**.
8. Select **Default**.
9. Adjust your settings.
10. If you want to preview the HTML template, click **Preview**. An e-mail is sent to your user and you can check the template you are customizing. If you want to exchange the logo, make sure that the logo is saved on the server to grant access whenever e-mails are automatically sent.
11. Click **Save**.

You have customized the default HTML e-mail template.





16.2.10.4 Customize HTML templates for multiple locales

You can customize the templates for user-defined notifications. Variables (page 217) may be used to personalize the content of a notification of ARIS Administration. Variables can be used in both notification subject and body.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **User-defined notifications**.
5. Click a category.
6. Click  **Upload**. The corresponding dialog opens.
7. Enable **Advanced template configuration**.
8. Select a locale.
9. Adjust your settings.
10. If you want to preview the HTML template, click **Preview**. An e-mail is sent to your user and you can check the template you are customizing. If you want to exchange the logo, make sure that the logo is saved on the server to grant access whenever e-mails are automatically sent.
11. Click **Save**.

You have customized the HTML e-mail template for a locale. If an e-mail is sent to a user and a notification language is specified for this user, the corresponding HTML template is now used for this language.

16.2.10.5 Properties for user-defined notifications

You can customize the user-defined notifications (page 200) as required.

Variables (page 217) may be used to personalize the content of a notification of ARIS Administration. Variables can be used in both notification subject and body.

USERS

Key	Description	Valid input	Example
com.aris.umc.notification.userCreated.message	Notify about creation Specifies whether users are to be notified after they have been created.	true, False	
com.aris.umc.notification.userCreated.subject	User created - Subject Subject of the notification that is sent when a user has been created.	String	
com.aris.umc.notification.userCreated.message	User created - Message Specifies the text of the notification that is sent when a user has been created.	String	
com.aris.umc.notification.userCreated.template	User created - HTML template Specifies the HTML template used for the notification that is sent when users are notified that they have been created. The template must have been uploaded previously.		

Key	Description	Valid input	Example
com.aris.umc.notification.userDisabled.enabled	<p>Notify about deactivation</p> <p>Specifies whether users are to be notified after they have been deactivated. For a notification to be sent, the Process Governance license privilege must be revoked from a user.</p>	True, False	
com.aris.umc.notification.userDisabled.subject	<p>User deactivated - Subject</p> <p>Specifies the subject of the notification that is sent when a user has been deactivated.</p>	String	
com.aris.umc.notification.userDisabled.message	<p>User deactivated - Message</p> <p>Specifies the text of the notification that is sent when a user has been deactivated.</p>	String	
com.aris.umc.notification.userDisabled.template	<p>User deactivated - HTML template</p> <p>Specifies the HTML template used for the notification that is sent when users are notified that they have been deactivated. The template must have been uploaded previously.</p>		
com.aris.umc.notification.userEnabled.enabled	<p>Notify about activation</p> <p>Specifies whether users are to be notified after they have been activated. For a notification to be sent, the Process Governance license privilege must be assigned to a user.</p>	True, False	

Key	Description	Valid input	Example
com.aris.umc.notification.userEnabled.subject	User activated - Subject Specifies the subject of the notification that is sent when a user has been activated.	String	
com.aris.umc.notification.userEnabled.message	User activated - Message Specifies the text of the notification that is sent when a user has been activated.	String	
com.aris.umc.notification.userEnabled.template	User activated - HTML template Specifies the HTML template used for the notification that is sent when users are notified that they have been activated. The template must have been uploaded previously.	String	

PASSWORDS

Key	Description	Valid input	Example
com.aris.umc.notification.passwordChanged.enabled	Notify about password change Specifies whether users are to be notified after their password has been changed.	True, False	
com.aris.umc.notification.passwordChanged.subject	Password change - Subject Specifies the subject of the notification that is sent when a password has been changed.	String	

Key	Description	Valid input	Example
com.aris.umc.notification.passwordChanged.message	Password change - Message Specifies the text of the notification that is sent when a password has been changed.	String	
com.aris.umc.notification.passwordChanged.template	Password change - HTML template Specifies the HTML template used for the notification that is sent when a user is to be notified about a password change. The template must have been uploaded previously.		
com.aris.umc.notification.passwordReset.enabled	Notify about password reset Specifies whether users are to be notified after their password has been reset.	True, False	
com.aris.umc.notification.passwordReset.subject	Password reset - Subject Specifies the subject of the notification that is sent when a password has been reset.	String	
com.aris.umc.notification.passwordReset.message	Password reset - Message Specifies the text of the notification that is sent when a password has been reset.	String	
com.aris.umc.notification.passwordReset.template	Password reset - HTML template Specifies the HTML template used for the notification that is sent when a user is to be notified about a password reset. The template must have been uploaded previously.		

Key	Description	Valid input	Example
com.aris.umc.notification.passwordResetRequested.enabled	Notify about password reset request Specifies that users are to be notified if they have requested a password reset.	True, False	
com.aris.umc.notification.passwordResetRequested.subject	Password reset request - Subject Specifies the subject of the notification that is sent when a user has requested a password reset.	String	
com.aris.umc.notification.passwordResetRequested.message	Password reset request - Message Specifies the text of the notification that is sent when a user has requested a password reset.	String	
com.aris.umc.notification.passwordResetRequested.template	Password reset request - HTML template Specifies the HTML template used for the notification that is sent when a user has requested a password reset. The template must have been uploaded previously.		

LICENSES

Key	Description	Valid input	Example
com.aris.umc.notification.licenseExpired.enabled	Notify about license expiration Specifies whether administrators with the License management privilege are to be notified when a license has expired.	True, False	True

Key	Description	Valid input	Example
com.aris.umc.notification.license Expired.subject	License has expired - Subject Specifies the subject of the notification that is sent when a license has expired.	String	
com.aris.umc.notification.license Expired.message	License has expired - Message Specifies the text of the notification that is sent when a license has expired.	String	
com.aris.umc.notification.license Expired.template	License has expired - HTML template Specifies the HTML template used for the notification that is sent when an administrator is to be notified that a license has expired. The template must have been uploaded previously.		
com.aris.umc.notification.license Expiring.enabled	Notify before license expiration Specifies whether administrators with the License management privilege are to be notified when a license is about to expire.	True, False	True
com.aris.umc.notification.license Expiring.threshold	Days before expiration Specifies how many days before license expiration a notification is sent.	Integer > 0	14
com.aris.umc.notification.license Expiring.subject	License will expire soon - Subject Specifies the subject of the notification that is sent when a license is about to expire.	String	

Key	Description	Valid input	Example
com.aris.umc.notification.license Expiring.message	License will expire soon - Message Specifies the text of the notification that is sent when a license is about to expire.	String	
com.aris.umc.notification.license Expiring.template	License will expire soon - HTML template Specifies the HTML template used for the notification that is sent when an administrator is to be notified that a license will soon expire. The template must have been uploaded previously.		
com.aris.umc.notification.license SeatsConsumed.enabled	Notify about license exhaustion Specifies whether administrators with the License management privilege are to be notified when the total number of logins allowed for the license is reached.	True, False	True
com.aris.umc.notification.license SeatsConsumed.threshold	Remaining license seats Defines how many license seats are allowed to be left before a notification is sent to inform users about the upcoming expiration of a license. In the case of named licenses, a notification is sent as soon as only the specified number of licenses are left from the total number of licenses available. In the case of concurrent licenses, a notification is sent as soon as only the specified number of logins are left.	Integer > 0	5

Key	Description	Valid input	Example
com.aris.umc.notification.licenseSeatsConsumed.subject	License exhaustion - Subject Specifies the subject of the notification that is sent when the total number of logins allowed for the license is reached.	String	
com.aris.umc.notification.licenseSeatsConsumed.message	License exhaustion - Message Specifies the text of the notification that is sent when a license has expired.	String	
com.aris.umc.notification.licenseSeatsConsumed.template	License exhaustion - HTML template Specifies the HTML template used for the notification that is sent when an administrator is to be notified that a license will soon expire. The template must have been uploaded previously.		

TENANTS

Key	Description	Valid input	Example
com.aris.umc.notification.tenantDeleted.enabled	Notify about deletion Specifies whether a notification is sent if a tenant was deleted.	True, False	True
com.aris.umc.notification.tenantDeleted.sendToAll.enabled	Notify all users about deletion Specifies whether a notification is to be sent to all users.	True, False	True
com.aris.umc.notification.tenantDeleted.subject	Tenant deleted - Subject Specifies the subject of the notification that is sent if a tenant was deleted.	String	

Key	Description	Valid input	Example
com.aris.umc.notification.tenantDeleted.message	Tenant deleted - Message Specifies the text of the notification that is sent if a tenant was deleted.	String	
com.aris.umc.notification.tenantDeleted.template	Tenant deleted - HTML template Specifies the HTML template used for the notification that is sent when an administrator is to be notified that a tenant has been deleted. The template must have been uploaded previously.		
com.aris.umc.notification.tenantDisabled.enabled	Notify about deactivation Specifies whether a notification is sent if a tenant was deactivated.	True, False	True
com.aris.umc.notification.tenantDisabled.sendToAll.enabled	Notify all users about deactivation Specifies whether a notification is sent to all users if a tenant was deactivated.	True, False	True
com.aris.umc.notification.tenantDisabled.subject	Tenant deactivated - Subject Specifies the subject of the notification that is sent if a tenant was deactivated.	String	
com.aris.umc.notification.tenantDisabled.enabled	Tenant deactivated - Message Specifies the text of the notification that is sent if a tenant was deactivated.	String	

Key	Description	Valid input	Example
com.aris.umc.notification.tenantDisabled.template	Tenant deactivated - HTML template Specifies the HTML template used for the notification that is sent when an administrator is to be notified that a tenant has been deactivated. The template must have been uploaded previously.		
com.aris.umc.notification.tenantEnabled.enabled	Notify about activation Specifies whether a notification is sent if a tenant was activated.	True, False	True
com.aris.umc.notification.tenantEnabled.sendToAll.enabled	Notify all users about activation Specifies whether a notification is sent to all users if a tenant was activated.	True, False	True
com.aris.umc.notification.tenantEnabled.subject	Tenant activated - Subject Specifies the subject of the notification that is sent if a tenant was activated.	String	
com.aris.umc.notification.tenantEnabled.message	Tenant activated - Message Specifies the text of the notification that is sent if a tenant was activated.	String	
com.aris.umc.notification.tenantEnabled.template	Tenant activated - HTML template Specifies the HTML template used for the notification that is sent when an administrator is to be notified that a tenant has been activated. The template must have been uploaded previously.		

MULTI-FACTOR AUTHENTICATION

Key	Description	Valid input	Example
com.aris.umc.notification.otpRequested.enabled	Notify about one-time password request Specifies whether users are to be notified if they have requested a one-time password.	True, False	
com.aris.umc.notification.otpRequested.subject	One-time password request - Subject Subject of the notification that is sent when a user has requested a one-time password.	String	
com.aris.umc.notification.otpRequested.message	One-time password request - Message Text of the notification that is sent when a user has requested a one-time password.	String	
com.aris.umc.notification.otpRequested.template	One-time password request - HTML template Specifies the HTML template used for the notification that is sent when a user has requested a one-time password. The template must have been uploaded previously.		
com.aris.umc.notification.otpSecretChanged.enabled	Notify about token secret change Specifies whether users are to be notified if their token secret has been changed.	True, False	
com.aris.umc.notification.otpSecretChanged.subject	Token secret change - Subject Subject of the notification that is sent when the token secret has been changed by a user.	String	

Key	Description	Valid input	Example
com.aris.umc.notification.otpSecretChanged.message	Token secret change - Message Text of the notification that is sent when the token secret has been changed by a user.	String	
com.aris.umc.notification.otpSecretChanged.template	Token secret change - HTML template Specifies the HTML template used for the notification that is sent when a user has changed the token secret. The template must have been uploaded previously.		

OAUTH

Key	Description	Valid input	Example
com.aris.umc.notification.signupCompleted.enabled	Notify about signup Specifies whether administrators are to be notified if a new user has signed up.	True, False	
com.aris.umc.notification.signupCompleted.subject	Signup complete - Subject Subject of the notification that is sent when a new user has signed up.	String	
com.aris.umc.notification.signupCompleted.message	Signup complete - Message Text of the notification that is sent when a new user has signed up.	String	

Key	Description	Valid input	Example
com.aris.umc.notification.signupCompleted.template	Signup complete - HTML template Specifies the HTML template used for the notification that is sent when a new user has signed up. The template must have been uploaded previously.		

16.2.10.6 Variables for user-defined notifications

Variables (page 217) may be used to personalize the content of a notification of ARIS Administration. Variables can be used in both notification subject and body. The following variables are supported:

TEXT NOTIFICATIONS:

- @tenant.name - Name of the tenant the user belongs to
- @user.login - Login of a user receiving notifications
- @user.givenName - First name of a user receiving notifications
- @user.lastName - Last name of a user receiving notifications
- @user.password - (New) password of a user receiving notifications

The following variables are supported for license-related events:

- @license.serial - Serial number of a license
- @license.productName - Name of a licensed product
- @license.expiry - Expiration date of a licensed product in the format YYYY-MM-DD

HTML NOTIFICATION

- \${tenant.name} - Name of the tenant the user belongs to
- \${user.login} - Login of a user receiving notifications
- \${user.givenName} - First name of a user receiving notifications
- \${user.lastName} - Last name of a user receiving notifications
- \${user.password} - (New) password of a user receiving notifications
- \${user.otpSecret} - Token secret of a user receiving notifications

The following variables are supported for license-related events:

- \${license.serial} - Serial number of a license
- \${license.productName} - Name of a licensed product
- \${license.expiry} - Expiration date of a licensed product in the format YYYY-MM-DD

16.2.11 Customize password policy






You can customize the password policies such as length or strength of a password depending on the use of special characters, numbers, etc.

You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **Password policy**.
5. Click a configuration category (page 219).
6. Click  **Edit**.
7. Adjust your settings.
8. Click  **Save**.

You have customized your system configuration.

16.2.12 Properties for password policies

You can customize your password policies (page 218) as required.

GENERAL

Key	Description
com.aris.umc.password.length.min	Minimum length Specifies the minimum length of a password. Valid input Integer > 0
com.aris.umc.password.length.max	Maximum length Specifies the maximum length of a password. Valid input 0 < Integer > 47
com.aris.umc.password.characters.lowercase.min	Minimum number of lowercase letters Specifies the minimum number of lowercase letters in a password. Valid input Integer > 0

Key	Description
com.aris.umc.password.character s.uppercase.allowed	Allow uppercase letters Specifies whether uppercase letters are allowed in a password. The default value is true . Valid input true, false Example True
com.aris.umc.password.character s.uppercase.min	Minimum number of uppercase letters Specifies the minimum number of uppercase letters in a password. Valid input Integer > 0
com.aris.umc.password.character s.numeric.allowed	Allow numbers Specifies whether numbers are allowed in a password. The default value is true . Valid input true, false Example True

Key	Description
com.aris.umc.password.character s.numeric.min	Minimum number of numbers Specifies the minimum number of numbers that must be contained in a password. Valid input Integer > 0
com.aris.umc.password.character s.special.allowed	Allow special characters Specifies whether special characters are allowed in a password. The default value is true . Valid input true, false Example True
com.aris.umc.password.character s.special.min	Minimum number of special characters Specifies the minimum number of special characters in a password. Valid input Integer > 0

Key	Description
com.aris.umc.password.character s.special.set	<p>Special characters</p> <p>Specifies which characters are special characters.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>*\$-+?&=!%{}/ _</p>
com.aris.umc.password.character s.sequential.allowed	<p>Allow sequential characters</p> <p>Specifies whether sequential characters are allowed in a password. This means a password can contain letters that follow each other in the alphabet, for example, abcfghsd. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>
com.aris.umc.password.character s.sequential.min	<p>Minimum number of sequential characters</p> <p>Specifies the minimum number of sequential characters in a password.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>3</p>

Key	Description
com.aris.umc.password.character s.repetitive.allowed	<p>Allow repetitive characters</p> <p>Specifies whether repetitive characters are allowed in a password. This means a password can contain the same letter in succession, for example, mmjfgbsd. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>
com.aris.umc.password.character s.repetitive.min	<p>Minimum number of repetitive characters</p> <p>Specifies the minimum number of repetitive characters in a password.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>3</p>

Key	Description
com.aris.umc.password.character s.context.allowed	<p>Allow context-related passwords</p> <p>Specifies whether context-related characters are allowed in a password. For example, if your username is JohnDoe, your password can be JohnIsBack. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>
com.aris.umc.password.character s.context.min	<p>Minimum number of context-related characters</p> <p>Specifies the minimum number of context-related characters in a password.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>3</p>
com.aris.umc.password.character s.common.allowed	<p>Allow commonly used passwords</p> <p>Specifies whether commonly used passwords are allowed. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>

Key	Description
com.aris.umc.password.character s.common.set	Common passwords Specifies a comma-separated list of common passwords. Valid input String Example myPassword,myLogin

EXPIRING PASSWORDS

Key	Description
com.aris.umc.password.expiry.act ive	Activate expiring passwords Specifies whether passwords are set to be valid only for a specific amount of time. This is defined for a single tenant. Once the password has expired, the user is directed to a Web site enabling the password to be changed. Thereafter, the user is redirected to the application. The default value is false . Valid input true, false Example False

Key	Description
com.aris.umc.password.expiry.days	Password lifetime Specifies the period of time in days after which a password expires. This is defined for a single tenant. Valid input Integer > 0

ADVANCED SETTINGS

Key	Description
com.aris.umc.password.change.forceAfterReset	Force change after reset Specifies whether a user must change the password if it was reset (and sent via e-mail). This is defined for a single tenant. The default value is false . Valid input true, false Example False

Key	Description
com.aris.umc.password.change.forceDifference	<p>Force different password</p> <p>Specifies whether the new password must differ from the old one. This is defined for a single tenant. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.password.change.forceOnFirstLogin	<p>Force change before first login</p> <p>Specifies whether a user must change the password upon first login. This is defined for a single tenant. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

Key	Description
com.aris.umc.password.reset.confirmation.active	<p>Activate reset confirmation</p> <p>Specifies whether a user must confirm a password reset. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>
com.aris.umc.password.reset.confirmation.ttl	<p>Link lifetime</p> <p>Specifies the time in minutes during which a user can click the emailed link to confirm the password.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>30</p>

16.2.13 SAML

SAML is an XML framework for exchanging authentication and authorization information. SAML provides functions to describe and transfer security-related information. ARIS supports SAML 2.0.





16.2.13.1 Customize SAML settings


ARIS supports SAML 2.0. You can customize the SAML settings for your ARIS system.


Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **SAML**.
5. Click a configuration category (page 231).
6. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

7. Adjust your settings.
8. Click  **Save**.

You have customized your system configuration.





16.2.13.2 Upload keystore file

You can upload the keystore file.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **SAML**.
5. Click **Keystore**.
6. Click  **Upload**. The dialog for uploading a file opens.
7. Select the relevant file.

You have uploaded a keystore file.





16.2.13.3 Upload truststore file

You can upload the truststore file.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **SAML**.
5. Click **Truststore**. You must have generated a truststore file.
6. Click  **Upload**. The dialog for uploading a file opens.
7. Select the relevant file.

You have uploaded a truststore file

16.2.13.4 SAML properties

You can configure SAML (page 229) as required.

You can change properties that are highlighted as cross-tenant properties only by using the ARIS Cloud Controller command-line tool. To change the settings, enter the following:

```
reconfigure umcadmin_<size of your installation, s, m, or l> JAVA-D<property name>="<value>"
```

Example

```
reconfigure umcadmin_m JAVA-Dcom.aris.umc.loadbalancer.url="https://myserver.com"
```

GENERAL

Key	Description
com.aris.umc.saml.active	<p>Use SAML</p> <p>Specifies whether an SAML-based login is allowed.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

Key	Description
com.aris.umc.saml.binding	<p>Binding</p> <p>Specifies the binding used for sending authentication requests to the identity provider. Defines how the redirecting of the authentication is performed. The options are Redirect or POST.</p> <p>Example</p> <p>POST</p>
com.aris.umc.saml.identity.provider.id	<p>Identity provider ID</p> <p>Specifies the ID of the identity provider.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.saml.service.provider.id	<p>Service provider ID</p> <p>Specifies the ID of the service provider.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.saml.identity.provider.sso.url	<p>Single sign-on URL</p> <p>Specifies the end point of the identity provider that is used for single sign-on.</p>
com.aris.umc.saml.identity.provider.logout.url	<p>Single logout URL</p> <p>Specifies the end point of the identity provider that is used for single log-out.</p>

SIGNATURE

Key	Description
com.aris.umc.saml.signature.assertion.active	<p>Enforce signing of assertions</p> <p>Enforces that SAML assertions must be signed. If set, all assertions received by the application must be signed. Assertions sent by the application are signed.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.saml.signature.request.active	<p>Enforce signing of requests</p> <p>Enforces that the SAML authentication requests must be signed. If set, all requests received by the application must be signed. Requests sent by the application are signed.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

Key	Description
com.aris.umc.saml.signature.response.active	<p>Enforce signing of responses</p> <p>Enforces that the SAML response must be signed. If set, all responses received by the application must be signed. Responses sent by the application are signed.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.saml.signature.metadata.active	<p>Enforce signing of metadata</p> <p>Enforces that the SAML metadata must be signed. If set, the service provider metadata file provided by the application is signed.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.saml.signature.algorithm	<p>Signature algorithm</p> <p>Specifies the algorithm for the signature. The algorithm can be selected from the list.</p> <p>Valid input</p> <p>String</p>

KEYSTORE

Key	Description
com.aris.umc.saml.keystore.location	Keystore Specifies the location of the keystore file used for validating SAML assertions. The keystore must have been uploaded previously.
com.aris.umc.saml.keystore.alias	Alias Specifies the alias name that is used to access the keystore. Valid input String
com.aris.umc.saml.keystore.password	Password Specifies the password that is used to access the keystore. Valid input String
com.aris.umc.saml.keystore.type	Type Specifies the type of the keystore to be used. The keystore type can be selected from a list. Valid input String Example JKB

TRUSTSTORE

Key	Description
com.aris.umc.saml.truststore.location	Truststore Specifies the location of the truststore file used for validating SAML assertions. The truststore must have been uploaded previously.
com.aris.umc.saml.truststore.alias	Alias Specifies the alias to be used for accessing the truststore. Valid input String
com.aris.umc.saml.truststore.password	Password Specifies the password to be used for accessing the truststore. Valid input String
com.aris.umc.saml.truststore.type	Type Specifies the type of the truststore. Valid input String Example JKB

USER ATTRIBUTES

Key	Description
com.aris.umc.saml.attribute.firstname	<p>First name</p> <p>Specifies the attribute name to be used for reading first names from a SAML assertion.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>John</p>
com.aris.umc.saml.attribute.lastname	<p>Last name</p> <p>Specifies the attribute name to be used for reading last names from a SAML assertion.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Doe</p>
com.aris.umc.saml.attribute.email	<p>E-mail address</p> <p>Specifies the attribute name to be used for reading e-mail addresses from a SAML assertion.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>jd@company.com</p>

Key	Description
com.aris.umc.saml.attribute.phone	<p>Telephone number</p> <p>Specifies the attribute name to be used for reading phone numbers from a SAML assertion.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>01234567</p>
com.aris.umc.saml.attribute.memberof	<p>Member of</p> <p>Attribute that references the groups of a user.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Main group</p>
com.aris.umc.saml.attribute.userdefined	<p>User-defined</p> <p>Comma-separated list of attributes to be imported as user-defined attributes of the user.</p>

ADVANCED SETTINGS

Key	Description
com.aris.umc.saml.login.mode.dn.active	Login using DN Specifies whether login is to be tried using the fully qualified name instead of the user name. Valid input true, false
com.aris.umc.saml.login.mode.keyword.active	Decompose DN Specifies whether the fully qualified name is to be decomposed. Valid input true, false
com.aris.umc.saml.login.mode.keyword.name	Keyword Specifies which part of the fully qualified name is to be used for login. Valid input true, false
com.aris.umc.saml.auth.context.class.refs	Authentication context classes Specifies the authentication context classes to request, meaning which strength of the authentication is defined. For example, you specify that users must use Kerberos if you define Microsoft® Windows as the Authentication context class and the Authentication context comparison as exact .

Key	Description
com.aris.umc.saml.auth.context.comparison	<p>Authentication context comparison</p> <p>Specifies the authentication context comparison to request, meaning you specify whether other authentication procedures are allowed or not. For example, you specify that users must use Kerberos if you define Microsoft® Windows as the Authentication context class and the Authentication context comparison as exact.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.saml.auth.nameid.format	<p>NameID format</p> <p>Specifies in which format the user ID is transferred to ARIS Administration.</p> <p>Valid input</p> <p>String</p>

Key	Description
com.aris.umc.saml.login.users.create	<p>Automatically create user</p> <p>Defines whether or not the user specified in the SAML assertion should be created automatically if the user does not already exist. The default value is false. The following restrictions apply to automatically created users:</p> <ul style="list-style-type: none">▪ The Login attribute is set to the name specified in the assertion.▪ The distinguished name attribute is set to the name specified in the assertion (only if the name is in an appropriate format).▪ A manual login is not possible if the password and e-mail attributes are not maintained. <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.saml.assertion.timeoffset	<p>Clock skew (in seconds)</p> <p>Specifies the time offset between identity provider and service provider in seconds. Assertions are accepted if they are received within the permitted time frame.</p> <p>Example</p> <p>60</p>
com.aris.umc.saml.service.provider.urls	<p>Allowed service provider URLs</p> <p>Comma-separated list of service provider URLs that are allowed to request that the user administration initiates the use of SSO.</p>

Key	Description
com.aris.umc.saml.assertion.ttl	<p>Assertion lifetime (in seconds)</p> <p>Specifies the maximum lifetime of a SAML assertion in seconds.</p> <p>Example</p> <p>10</p>
com.aris.umc.saml.service.provider.assertion.consumer.url.override	<p>Assertion Consumer Service URL</p> <p>Specifies that the Assertion Consumer Service URL used in SAML authentication requests can be overwritten. The URL must be specified in the format of http(s)://hostname/umc/rest/saml/itsso. If no specification is made, the URL is derived from the HTTP request.</p>
com.aris.umc.saml.tenant	<p>Default tenant</p> <p>Specifies the default tenant that is to be used for the SAML-based login.</p> <p>Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>default</p>





16.2.14 Customize security settings


You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.


Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **Security**.
5. Click a configuration category (page 244).
6. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

7. Adjust your settings.
8. Click  **Save**.

You have customized your system configuration.

16.2.15 Security properties

You can customize the security settings (page 243) as required.

You can change properties that are highlighted as cross-tenant properties only by using the ARIS Cloud Controller command-line tool. To change the settings, enter the following:

```
reconfigure umcadmin_<size of your installation, s, m, or l> JAVA-D<property name>="<value>"
```

Example

```
reconfigure umcadmin_m JAVA-Dcom.aris.umc.loadbalancer.url="https://myserver.com"
```

ACCOUNT LOCKOUT

Key	Description	Valid input	Example
com.aris.umc.authentication.lock.enabled	<p>Lock users after failed login attempts</p> <p>Specifies whether a user login is temporarily locked when a user causes too many failed logins. The default value is false.</p>	true, false	
com.aris.umc.authentication.lock.counter.limit	<p>Attempt limit</p> <p>Specifies the number of failed login attempts that are allowed before user login is locked.</p>	Integer > 0	
com.aris.umc.authentication.lock.ttl	<p>Lockout duration (in seconds)</p> <p>Specifies how long a user login is temporarily locked when a user causes too many failed logins. This is defined in seconds.</p>	Integer > 0	

Key	Description	Valid input	Example
com.aris.umc.authentication.lock.counter.ttl	<p>Lock counter duration (in seconds)</p> <p>Time that must elapse before the number of failed login attempts is reset. This is defined in seconds.</p>	Integer > 0	

USER SESSIONS

Key	Description	Valid input	Example
com.aris.umc.session.renewal.cache.size	<p>Session cache size</p> <p>Specifies how many session IDs are saved in the session renewal cache. When the cache is full, the least recently used sessions are removed. This is defined in seconds. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p>	Integer > 0	
com.aris.umc.session.renewal.cache.ttl	<p>Session cache lifetime (in seconds)</p> <p>Specifies the maximum duration in seconds that a renewed session remains in the session renewal cache. A session can be renewed at the earliest after this period of time. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p>	Integer > 0	

Key	Description	Valid input	Example
com.aris.umc.session.identifier.generator	Session ID generator Specifies the random number generator used for generating session IDs.	String	
com.aris.umc.session.identifier.length.min	Minimum length of session ID (in bytes) Specifies the minimum length of a session ID in bytes. For security reasons this value should not be less than 32.	Integer > 0	
com.aris.umc.session.identifier.length.max	Maximum length of session ID (in bytes) Specifies the maximum length of a session ID in bytes.	Integer > 0	
com.aris.umc.session.concurrent.max	Maximum concurrent sessions Specifies the maximum number of concurrent sessions that can be active for a single user. This does not apply to the arisservice and superuser users.	Integer > 0	

MULTI-FACTOR AUTHENTICATION

Key	Description	Valid input	Example
com.aris.umc.authentication.multiFactor.active	Use multi-factor authentication You can use multi-factor authentication only in API Portal. Specifies whether multi-factor authentication is required. The default value is false .	true, false	

Key	Description	Valid input	Example
com.aris.umc.authentication.multipactor.clockSkew	Clock skew intervals Specifies the clock skew in number of intervals. One-time passwords (OTPs) that are within the valid range [currentTimeStep - clock_skew, currentTimeStep + clock_skew] are permitted. This is defined in milliseconds. You can use multi-factor authentication only in API Portal.	Integer > 0	
com.aris.umc.authentication.multipactor.excludedUsers	Excluded users Specifies a comma-separated list of users for whom the multi-factor authentication is not required. You can use multi-factor authentication only in API Portal.	String	

ADVANCED SETTINGS

Key	Description	Valid input	Example
com.aris.umc.audit.enabled	<p>Generate user statistics</p> <p>Enables the generation of user statistics. The default value is false. If you specify this as true, the following properties for distinct user statistics are enabled as default:</p> <ul style="list-style-type: none"> ▪ Log authentication ▪ Log changes to configuration ▪ Log changes to licenses/privileges ▪ Log changes to users/user groups ▪ You can disable/enable the properties mentioned above. 	true, false	false
com.aris.umc.audit.log.auth.enabled	<p>Log authentication</p> <p>Enables authentication logging. The default value is true but this property is only enabled when Generate user statistics is specified as true. The following user statistics are logged and can be exported (page 58):</p> <ul style="list-style-type: none"> ▪ Login failed ▪ Login successful ▪ Logged out ▪ Logged out by administrator 	true, false	true

Key	Description	Valid input	Example
com.aris.umc.audit.log.conf.enabled	<p>Log changes to configuration</p> <p>Enables logging of changes to the configuration. The default value is true. The following user statistics are logged and can be exported (page 58):</p> <ul style="list-style-type: none"> ▪ Organizational chart deleted ▪ Organizational chart updated ▪ One-time password requested ▪ Password changed ▪ Password reset ▪ Password transferred between users ▪ Profile picture deleted ▪ Profile picture imported ▪ Privilege assigned ▪ Privilege assignment removed ▪ Configuration option changed ▪ Configuration file deleted ▪ Configuration file imported ▪ Data backup imported ▪ Tenant created ▪ Tenant deleted ▪ Tenant updated 	true, false	true

Key	Description	Valid input	Example
com.aris.umc.audit.log.license.privilege.enabled	<p>Log changes to licenses/privileges</p> <p>Enables logging of changes to licenses or privileges. The default value is true. The following user statistics are logged and can be exported (page 58):</p> <ul style="list-style-type: none">▪ License deleted▪ License imported▪ License consumed▪ License released▪ Violation of user group license limit▪ Violation of user license limit▪ Replace license file for tenant	true, false	true

Key	Description	Valid input	Example
com.aris.umc.audit.log.user.group.enabled	<p>Log changes to users/user groups</p> <p>Enables logging of changes to users or user groups. The default value is true. The following user statistics are logged and can be exported (page 58):</p> <ul style="list-style-type: none">▪ User created▪ User deleted▪ Escalation manager assignment removed▪ User group created▪ User group deleted▪ Group assigned to group▪ Group unassigned from group▪ User group updated▪ LDAP data imported▪ Synchronized with LDAP	true, false	true
com.aris.umc.audit.log.application.enabled	<p>Log application changes</p> <p>Enables logging of all changes to applications, regardless of whether they are internal or external. The default value is true.</p>		

Key	Description	Valid input	Example
com.aris.umc.authentication.sso.only	<p>Force SSO</p> <p>Specifies that only an SSO login is allowed. If this option is enabled no local users except local superuser and the system user can log in. Otherwise, the system would not be accessible at all in case of SSO errors or misconfiguration. The default value is false.</p>	true, false	false
com.aris.umc.authentication.sso.force.downloadclient.only	<p>Force SSO for ARIS Download Client</p> <p>If this option is enabled, a user must be logged in to the portal to be able to start ARIS Download Client. The default value is false.</p>	true, false	false
com.aris.umc.authentication.delay.min	<p>Minimum authentication delay (in milliseconds)</p> <p>Specifies the minimum delay that is added at each login. This is defined in milliseconds.</p>	Integer > 0	
com.aris.umc.authentication.delay.max	<p>Maximum authentication delay (in milliseconds)</p> <p>Specifies the maximum delay that is added at each login. This is defined in milliseconds.</p>	Integer > 0	
com.aris.umc.otp.active	<p>Use OTPs</p> <p>Specifies whether or not the generation of one-time passwords (OTPs) is allowed.</p>	true, false	
com.aris.umc.otp.ttl	<p>Lifetime (in seconds)</p> <p>Specifies the lifetime of a one-time password (OTP) in seconds. Passwords become invalid after this time period at the latest.</p>		

Key	Description	Valid input	Example
com.aris.ums.license.distribution.handling	License pools at user group-level Specifies that license pools are assigned at the user group level (page 44). If this option is enabled, licenses must not be assigned to users directly, but are to be assigned via user groups only.	true, false	false
com.aris.ums.user.statistics.backup	User statistics in backup Specifies that the user statistics are part of the backup. The default value is true .	true, false	false
com.aris.ums.user.statistics.persistent.days	Purge user statistics generated before (in days) Specifies the number of days user statistics must be available.	Integer	365
com.aris.ums.applications.registration	Application registration Specifies a comma-separated list of internal applications for registering an application. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual .		





16.2.16 Customize SMTP settings


You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.


Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **SMTP**.
5. Click a configuration category (page 255).
6. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

7. Adjust your settings.
8. Click  **Save**.

You have customized your system configuration.

16.2.17 SMTP properties

You can configure SMTP (page 254) as required.

You can change properties that are highlighted as cross-tenant properties only by using the ARIS Cloud Controller command-line tool. To change the settings, enter the following:

```
reconfigure umcadmin_<size of your installation, s, m, or l> JAVA-D<property name>="<value>"
```

Example

```
reconfigure umcadmin_m JAVA-Dcom.aris.umc.loadbalancer.url="https://myserver.com"
```

CONNECTION

Key	Description
com.aris.umc.notification.smtp.host	<p>Host name</p> <p>Specifies the host name or IP address of the SMTP server. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>localsmtp.my.corp.softwareag.com</p>

Key	Description
com.aris.umc.notification.smtp.port	<p>Port</p> <p>Specifies the port for the SMTP server.</p> <p>Valid input</p> <p>Integer greater than or equal to 0, but less than or equal to 65535</p>
com.aris.umc.notification.sender	<p>Sender address</p> <p>Specifies the sender address for notifications. This must be a valid e-mail address.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.notification.type	<p>E-mail format</p> <p>Specifies the default type used for sending notifications.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.notification.language	<p>Default language</p> <p>Specifies the default language in which notifications are sent. If this property is not defined, the server operating system language is used. If a user prefers a different locale, this locale is given preference. Otherwise, the global settings are considered.</p> <p>Valid input</p> <p>en</p>

Key	Description
com.aris.umc.notification.smtp.authentication	Use authentication Specifies whether authentication to the SMTP server is to be used. Valid input true, false
com.aris.umc.notification.smtp.userName	User name Specifies the user name that is used for authentication. Valid input String
com.aris.umc.notification.smtp.password	Password Specifies the password that is used for authentication to the SMTP server. Valid input String Example smtppassword

Key	Description
com.aris.umc.notification.smtp.ssl	<p>Use SSL</p> <p>Specifies whether TLS is to be used for the connection to the SMTP server.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.notification.smtp.ssl.mode	<p>SSL mode</p> <p>Specifies the method to be used for a trusted connection. STARTTLS or SSL can be used. STARTTLS transforms a connection that was originally untrusted into an encrypted connection without requiring a specific port for the trusted connection. SSL establishes a trusted connection with a dedicated port immediately.</p> <p>Valid input</p> <p>STARTTLS, SSL</p> <p>Example</p> <p>STARTTLS</p>
com.aris.umc.notification.smtp.timeout	<p>Connection timeout (in milliseconds)</p> <p>Specifies the duration after which the attempt to connect to the SMTP server is canceled. This is defined in milliseconds.</p> <p>Valid input</p> <p>Integer > 0</p>

ADVANCED SETTINGS

Key	Description
com.aris.umc.notification.debug	Debug output Activates debugging output. Valid input true, false
com.aris.umc.notification.smtp.retry.count	Number of retries Specifies the number of retries for sending notifications. Valid input Integer > 0
com.aris.umc.notification.smtp.retry.sleep.min	Minimum wait time (in milliseconds) Specifies the minimum wait time between the retries. This is defined in milliseconds. Valid input Integer > 0
com.aris.umc.notification.smtp.retry.sleep.max	Maximum wait time (in milliseconds) Specifies the maximum wait time between the retries. This is defined in milliseconds. Valid input Integer > 0

Key	Description
com.aris.umc.notification.smtp.sendrate	<p>Send rate (per second)</p> <p>Specifies the maximum number of messages sent per second. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.umc.notification.smtp.replyto	<p>Reply-to addresses</p> <p>Specifies a comma-separated list of reply-to addresses.</p>
com.aris.umc.notification.threads	<p>Number of threads</p> <p>Specifies the maximum number of threads that are used for sending notifications. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.umc.notification.queue	<p>Maximum queue length</p> <p>Specifies the maximum number of notifications allowed in a send queue. If the send queue is too full, all subsequent notifications are refused. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p>






16.2.18 Customize user settings

You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **Users**.
5. Click a configuration category (page 262).
6. Click  **Edit**.
7. Adjust your settings.
8. Click  **Save**.

You have customized your system configuration.

16.2.19 Properties for user settings

You can customize the configuration for users (page 261) as required.

GENERAL

Key	Description
com.aris.umc.users.email.required	E-mail address required Specifies whether the E-mail address box must be specified for a user. Valid input true, false
com.aris.umc.users.email.validation.active	Validate e-mail address Specifies whether a check is performed when entering the e-mail address of a user to determine whether the e-mail address is valid. Valid input true, false
com.aris.umc.users.name.length.max	Maximum login name length Specifies the maximum length of the login names. Valid input Integer > 0

Key	Description
com.aris.umc.collaboration.picture.size.max	<p>Maximum picture size (in bytes)</p> <p>Specifies the maximum size of a profile picture in bytes. The default setting is 1048576 bytes.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>1048576</p>
com.aris.umc.session.system.ttl	<p>Initial session duration (in minutes)</p> <p>Specifies the initial duration of a system user session in minutes.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.umc.session.system.ttl.max	<p>Maximum session duration (in minutes)</p> <p>Specifies the maximum duration of a system user session in minutes.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.umc.impersonation.targets	<p>Impersonation target users</p> <p>Specifies the users for which you want to allow impersonation (page 147).</p> <p>Valid input</p> <p>String</p>

Key	Description
com.aris.umc.default.group	<p>Default user group name</p> <p>Specifies an existing user group as default user group to which all users created afterwards will be assigned.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.chart.display.technicalUsers.enabled	<p>Display technical users</p> <p>Specifies whether or not user statistics and charts are also displayed for technical users such as system, arisservice, superuser, and guest.</p> <p>Valid input</p> <p>true, false</p>

ARISSERVICE

Key	Description
com.aris.umc.users.service.create	<p>Generate, if not available</p> <p>Specifies whether the user arisservice is generated at startup, if not yet available. If you explicitly delete (page 25) this user, the Generate, if not available option is disabled and the user is no longer generated at startup.</p> <p>Valid input</p> <p>true, false</p>

Key	Description
com.aris.umc.users.service.name	User name Specifies the login name of the user arisservice . Valid input String
com.aris.umc.users.service.email	E-mail address Specifies the e-mail address of the user arisservice . Valid input String
com.aris.umc.users.service.password	Initial password Specifies the initial password of the user arisservice . Valid input String

GUEST

Key	Description
com.aris.umc.users.guest.create	<p>Generate, if not available</p> <p>Specifies whether the user guest is generated at startup, if not yet available. If you explicitly delete (page 25) this user, the Generate, if not available option is disabled and the user is no longer generated at startup.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.users.guest.name	<p>User name</p> <p>Specifies the login name of the user guest.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.users.guest.email	<p>E-mail address</p> <p>Specifies the e-mail address of the user guest.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.users.guest.password	<p>Initial password</p> <p>Specifies the initial password of the user guest.</p> <p>Valid input</p> <p>String</p>

Key	Description
com.aris.umc.users.guest.allow.automato.login	Automatically log in visitors Specifies that visitors are automatically logged in as a guest when accessing the ARIS Connect portal. Valid input true, false

SUPERUSER

Key	Description
com.aris.umc.users.admin.name	User name Specifies the login name of the administrator in ARIS Administration. You cannot delete this user. Valid input String
com.aris.umc.users.admin.email	E-mail address Specifies the e-mail address of the administrator. Valid input String
com.aris.umc.users.admin.password	Initial password Specifies the initial password of the administrator in ARIS Administration. Valid input String

SYSTEM

Key	Description
com.aris.umc.users.system.create	<p>Generate, if not available</p> <p>Specifies whether the user system is generated at startup, if not yet available. If you explicitly delete (page 25) this user, the Generate, if not available option is disabled and the user is no longer generated at startup.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.users.system.name	<p>User name</p> <p>Specifies the login name of the user system.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.users.system.email	<p>E-mail address</p> <p>Specifies the e-mail address of the user system.</p> <p>Valid input</p> <p>String</p>
com.aris.umc.users.system.password	<p>Initial password</p> <p>Specifies the initial password of the user system.</p> <p>Valid input</p> <p>String</p>

Key	Description
com.aris.umc.session.system.ttl	Initial session duration (in minutes) Specifies the initial life span of the system user session in minutes. Valid input Integer > 0
com.aris.umc.system.session.ttl. max	Maximum session duration (in minutes) Specifies the maximum life span of the system user session in minutes. Valid input Integer > 0

16.2.20 SCIM

System for **C**ross-**D**omain **I**ntity **M**anagement (SCIM) is designed to facilitate the management of user identities in cloud-based applications and services. ARIS supports SCIM 2.0.

16.2.20.1 Customize SCIM settings






You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration. ARIS supports SCIM with SAML 2.0.

We recommend that you use your own local user who has the **Technical configuration administrator** function privilege and the **User administrator** function privilege. This user can generate a bearer token and forward it together with the SCIM end point URL (page 274) to the SCIM administrator.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **SCIM**.
5. Click a configuration category (page 274).
6. Click  **Edit**.
7. Adjust your settings.
8. Click  **Save**.

You have customized your system configuration.

16.2.20.2 Generate bearer token





If you suspect that your bearer token is no longer safe, you can generate a new bearer token and hand it over to your SCIM administrator.

We recommend that you use your own local user who has the **Technical configuration administrator** function privilege and the **User administrator** function privilege. This user can generate a bearer token and forward it together with the SCIM end point URL (page 274) to the SCIM administrator.

Prerequisite

- You have the **User administrator** function privilege.
- SCIM is enabled and correctly configured in **ARIS Administration > Configuration > User management > SCIM**.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **User management**. The list of users is displayed.
3. Click your user. The bearer token is always user-specific. In principle one bearer token is sufficient system-wide.
4. Click **SCIM bearer token**.
5. Click  **Generate bearer token**. The dialog opens.
6. Click **OK** to confirm.

The new bearer token is generated.

Click **Copy** to copy the bearer token to the clipboard to hand it over to your SCIM administrator so that it can be imported.




16.2.20.3 Copy bearer token to clipboard

You can copy the bearer token to the clipboard to hand it over to your SCIM administrator so that he can import it.

Prerequisite

- You have the **User administrator** function privilege.
- SCIM is enabled and correctly configured in **ARIS Administration > Configuration > User management > SCIM**.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **User management**. The list of users is displayed.
3. Click your user. The bearer token is always user-specific. In principle one bearer token is sufficient system-wide.
4. Click **Copy** to copy the bearer token to the clipboard.

You can hand over the bearer token to your SCIM administrator so that he can import it.




16.2.20.4 Delete bearer token

You can delete a bearer token.

Prerequisite

- You have the **User administrator** function privilege.
- SCIM is enabled and correctly configured in **ARIS Administration > Configuration > User management > SCIM**.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **User management**. The list of users is displayed.
3. Click your user. The bearer token is always user-specific. In principle one bearer token is sufficient system-wide.
4. Click **SCIM bearer token**.
5. Click **Delete**.

The bearer token is deleted.






16.2.20.5 Specify SCIM client

You can specify a SCIM client.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **SCIM**.
5. Click a **SCIM client**.
6. Click  **Edit**.
7. Adjust your settings.
8. Click  **Save**.

You have specified a SCIM client.

16.2.20.6 SCIM properties

You can configure SCIM as required.

GENERAL

Key	Description
com.aris.umc.scim.active	<p>Use SCIM</p> <p>Enables SCIM support for User Management.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.scim.endpoint.url	<p>SCIM end point URL</p> <p>Specifies the end point URL used for SCIM. You cannot change this property.</p> <p>Valid input</p> <p><loadbalancerurl>/umc/scim/v2/{tenant}</p>

Key	Description
com.aris.umc.scim.basic.auth.active	<p>Basic authentication</p> <p>Enables the authentication scheme using the HTTP basic standard. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>
com.aris.umc.scim.bearer.token.active	<p>Bearer token</p> <p>Enables the authentication scheme using the bearer token standard. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>
com.aris.umc.scim.token.expiry.day	<p>Token lifetime (in days)</p> <p>Specifies that the bearer token will expire after this period of time in days.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>365</p>

ADVANCED SETTINGS

Key	Description	Valid input	Example
com.aris.umc.scim.service.provider.advance.settings.patch.support	<p>Patch support</p> <p>The patch support is an optional server functionality that enables clients to update one or more attributes of a SCIM resource, for example a user or a user group, using a sequence of operations to add, remove, or replace values. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>	True, False	True
com.aris.umc.scim.service.provider.advance.settings.change.password.support	<p>Change password support</p> <p>Enables the support for changing a user password. This means that if a user changes the password in the SCIM system, the password is also changed for ARIS. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>	True, False	False

Key	Description	Valid input	Example
com.aris.umc.scim.service.provider.filter.support	<p>Filter support</p> <p>Specifies that clients can discover the filter capabilities of the service provider. Clients use the Filter attribute of the service provider's configuration end point. If filtering is enabled, not all users or user groups are transferred to ARIS, but only a subset. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>	True, False	True
com.aris.umc.scim.user.profile.photo.support	<p>Profile picture support</p> <p>Specifies whether a profile picture is supported. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>	True, False	False

SCIM CLIENT

Key	Description	Valid input	Example
com.aris.umc.scim.connection.enabled	<p>Provisioning</p> <p>Specifies whether the synchronization of users or user groups for the configured application is enabled. The default value is false.</p> <p>Provisioning and re-provisioning from the SCIM client</p> <p>A valid re-provisioning scenario is that users can be moved from the SCIM client to the SCIM server using the SCIM provisioning user interface. You must use the SCIM provisioning user interface to remove users from the SCIM server. You must use the SCIM provisioning user interface to add these users again to the SCIM server.</p> <p>An invalid re-provisioning scenario is that users can be moved from the SCIM client to the SCIM server using the SCIM provisioning user interface. If the administrator logs into the SCIM server itself and deletes all users from the SCIM server but the list of associated users is still maintained in the SCIM client system. This system does not know that users have been deleted from the SCIM server. Therefore, if the administrator wants to delete users directly in the server, the administrator must remove these users from the SCIM provisioning interface and add these users again using the SCIM provisioning interface. The default value is false.</p>	True, False	False

Key	Description	Valid input	Example
com.aris.umc.scim.connection.name	<p>Connection name</p> <p>Specifies the connection name used for identifying the application with which the user accounts are synchronized.</p>	String	myconnection
com.aris.umc.scim.connection.provision.mode	<p>Provisioning mode</p> <p>Specifies whether the creation and synchronization of user accounts based on user and group assignments is performed manually or automatically. The default value is Manual.</p>	Manual, Automatic	Manual
com.aris.umc.scim.connection.url	<p>Connection URL</p> <p>Specifies the connection string used to communicate with the SCIM services.</p>	URL	https://myserver.com
com.aris.umc.scim.connection.secret.token	<p>Secret token</p> <p>Is used to access the SCIM services to synchronize the user accounts.</p>	String	37283011-bd3e-4efe-8ed4-5f207b094453
com.aris.umc.scim.connection.provision.options	<p>Objects for provisioning</p> <p>Specifies which objects are synchronized. The default value is true.</p>	True, False	True
com.aris.umc.scim.connection.user.provision.actions	<p>Supported user actions</p> <p>Specifies what user actions are supported. The default value is true.</p>	True, False	True

Key	Description	Valid input	Example
com.aris.umc.scim.connection.group.provision.actions	Supported group actions Specifies what group actions are supported. The default value is true .	True, False	True
com.aris.umc.scim.connection.user.email.as.username	Use e-mail address as the user name Specifies that the e-mail address is used as the user name. If you want to use this option, the e-mail addresses must be unambiguous. Otherwise, all actions performed for users or user groups will fail. The default value is false .	True, False	False






16.2.21 Customize Application switcher

You can enable (page 282) a specific ARIS Process Mining system and specify the relevant URL.

Prerequisite

- You have the **User administrator** function privilege.
- You have an ARIS Process Mining system running.
- You have the **ARIS Process Mining administrator** function privilege.
- You have ARIS Process Mining registered as a trustworthy application.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **User management**. The list of users is displayed.
3. Click the arrow next to **Application switcher**.
4. Click **General**.
5. Click  **Edit**.
6. Enable **Link to ARIS Process Mining**.
7. Enter the relevant URL.
8. Enter the tenant.
9. Click  **Save**.

You have enabled and configured ARIS Process Mining.

16.2.22 Application switcher properties

You can enable ARIS Process Mining and specify (page 281) the URL to a specific ARIS Process Mining system.

Key	Description
com.aris.umc.process.mining.active	<p>Enable link to ARIS Process Mining</p> <p>Enables the ARIS Process Mining support for the user management. If this option is enabled, you can enter the URL of ARIS Process Mining. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.process.mining.endpoint	<p>ARIS Process Mining URL</p> <p>Specifies the end point URL of a specific ARIS Process Mining system.</p> <p>Valid input</p> <p>URL</p> <p>Example</p> <p>http://www.myserver.com</p>

Key	Description
com.aris.umc.process.mining.tenant	<p data-bbox="631 258 2078 363">Tenant Specifies the ARIS Process Mining tenant name.</p> <p data-bbox="631 370 2078 475">Valid input String</p> <p data-bbox="631 481 2078 596">Example mytenantname</p>

16.2.23 What is ARIS Process Mining?

Process Mining is the visualization and analysis of business processes on the basis of event logs using algorithms and mathematical methods.






16.2.24 Customize OAuth 2.0 settings

You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration. ARIS supports OAuth 2.0.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Activate **User Management**.
4. Click the arrow next to **OAuth 2.0**.
5. Click a configuration category.
6. Click  **Edit**.
7. Adjust your settings.
8. Click  **Save**.

You have customized your system configuration.

16.2.25 OAuth 2.0 properties

You can configure OAuth 2.0 as required.

GENERAL

Key	Description
com.aris.umc.oauth2.active	<p>Use OAuth2.0</p> <p>Enables OAuth2.0 support for the user management. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.oauth2.client.id	<p>Client ID</p> <p>Specifies the client ID of the application.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>ARIS Process Mining</p>
com.aris.umc.oauth2.client.secret	<p>Client secret</p> <p>Specifies the client secret of the application.</p>

Key	Description
com.aris.umc.oauth2.well.known.url	Well-known URL Specifies the well-known URL of the application Valid input URL Example http://www.myserver.com
com.aris.umc.oauth2.authorization.endpoint	Authorization end point Specifies the authorization end point of the application.
com.aris.umc.oauth2.authorization.endpoint	Access token end point Specifies the access token end point of the application.
com.aris.umc.oauth2.user.info.endpoint	User information end point Specifies the user information end point.
com.aris.umc.oauth2.refresh.token.endpoint	Refresh token endpoint Specifies the endpoint for the refresh token. The refresh token is used to receive a new access token if the old token of the application has expired.
com.aris.umc.oauth2.create.user.enabled	Create user Supports user creation.

USER ATTRIBUTES

Key	Description
com.aris.umc.oauth2.attribute.user.name	Name Specifies the Name OAuth2.0 user attribute.
com.aris.umc.oauth2.attribute.first.name	First name Specifies the First name OAuth2.0 user attribute.
com.aris.umc.oauth2.attribute.last.name	Last name Specifies the Last name OAuth2.0 user attribute.
com.aris.umc.oauth2.attribute.email.address	E-mail address Specifies the E-mail address OAuth2.0 user attribute.
com.aris.umc.oauth2.attribute.telephone.number	Telephone number Specifies the Telephone number OAuth2.0 user attribute.
com.aris.umc.oauth2.attribute.member.of	Member of Specifies the Member of OAuth2.0 user attribute.
com.aris.umc.oauth2.attribute.user.defined	User-defined Specifies the User-defined OAuth2.0 user attribute.

16.3 Configure Document storage

You can customize general settings of ARIS document storage.




16.3.1 Import configuration

You can import configurations, which were, for example, exported from a different tenant, into any tenant or installation and use them there. This is an easy way to specify properties that are valid for all tenants on all tenants. This includes, for example, infrastructure settings, the configuration of third-party document management systems, or quota and restrictions settings. We recommend that you backup (page 289) your existing configuration before you import a configuration in case that the imported configuration does not meet your expectations.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click  **Import configuration file**.

The **Import configuration file** dialog opens. Navigate to the location where the configuration file is stored and import it. The new configuration is active immediately and no system restart is required.



16.3.2 Export configuration

You can export configurations in order to import them into any tenant or installation and use them there. This is an easy way to specify properties that are valid for all tenants on all tenants.

Prerequisite

- You have the **Technical configuration administrator** function privilege.
- You have allowed pop-ups for the pages of ARIS Administration.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click  **Export current configuration as a file**.

You can save the configuration file of ARIS document storage at the relevant location for further use.





16.3.3 Customize infrastructure settings

You can customize the infrastructure for your document storage, for example, the path for mobile uploads.


Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click **Infrastructure**. To configure advanced settings, click the arrow next to **Infrastructure** and click **Advanced settings**.
5. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

6. Adjust your settings.
7. Click  **Save**.

You have customized your document storage configuration (page 290).

16.3.4 Infrastructure properties

You can configure the infrastructure (page 289) for your document storage.

Properties that are highlighted as cross-tenant properties (🔑) can only be changed using ARIS Cloud Controller Command-line Tool (ACC). To change these settings enter the following:

```
reconfigure adsadmin_<size of your installation, s, m, or l> JAVA-D<property name>="<value>"
```

Example

```
reconfigure adsadmin_m JAVA-Dcom.aris.ads.thumbnails.queue.size="40"
```

Key	Description
com.aris.ads.filesystem.active	<p>Enable use of file share</p> <p>Specifies whether a network share or a local directory is used for storing document content. If enabled, only metadata is stored in the ARIS document storage database. The default value is true. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>
com.aris.ads.filesystem.path	<p>Path to the file share</p> <p>Path to a network share or a local directory where the document content is stored. If enabled, in distributed systems, all ARIS document storage instances must have access in the same way to this</p>

Key	Description
	<p>share or local directory. You must enter the network share in the following form: \\<servername>\<directory>, for example, \\myServer\data. If you leave the preconfigured path, all data is stored in the local file system under <ARIS installation directory>\server\bin\work\work_adsadmin_m\data. You can use an absolute path to the local file system as well, for example, C:\docdata. The default value is true. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>
com.aris.ads.audit.enabled	<p>Generate usage statistics</p> <p>Enables the generation of usage statistics. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>
com.aris.ads.anonymous.access.allowed	<p>Allow anonymous access by link</p> <p>Specifies that API Portal allows users to anonymously access all documents by the corresponding document link. The default value is true. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool</p>

Key	Description
	<p>manual.</p> <p>Valid input true, false</p> <p>Example true</p>
com.aris.ads.link.display.document.inline	<p>Display document content in the browser</p> <p>Specifies whether the content of a document is displayed in the browser by default. If displaying the content in the browser is not possible or the option is disabled, the document is downloaded. The default value is false.</p> <p>Valid input true, false</p> <p>Example false</p>

Key	Description
com.aris.ads.thumbnails.size	<p>Thumbnail width (in pixels)</p> <p>If the picture width is smaller than the thumbnail width specified, no thumbnail is displayed for this picture. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>160</p>
com.aris.ads.thumbnails.thread.count	<p>Maximum number of parallel scaling threads</p> <p>Specifies the maximum number of parallel threads for scaling document thumbnails.</p>
com.aris.ads.mobile.upload.path	<p>Folder for ARIS API uploads</p> <p>Specifies the path where to store files uploaded from mobile devices.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>/mobileuploads</p>

Key	Description
com.aris.ads.migration.skip	<p>Skip migration</p> <p>Specifies that data migration is to be skipped when the application is started for the first time after an update. The default value is false. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>
com.aris.ads.ignore.invalid.dms.config	<p>Do not validate configuration</p> <p>Specifies that the migration process ignores corrupt document management system configurations. The default value is false. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>

Key	Description
com.aris.ads.page.size	<p>Page size (default)</p> <p>Number of items that are retrieved by a single query. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>2500</p>
com.aris.ads.page.size.max	<p>Page size (max)</p> <p>Maximum number of items that can be retrieved by a single query. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>5000</p>
com.aris.ads.mobile.upload.path	<p>Read timeout (in milliseconds)</p> <p>Specifies the read timeout in milliseconds.</p> <p>Valid input</p> <p>Integer > 0</p>

Key	Description
com.aris.ads.dao.statistics.enabled	<p>Collect database statistics</p> <p>Collects statistics (for example, on query execution times) for all database queries. The default value is true. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>true, false</p>
com.aris.ads.config.cache.ttl	<p>Configuration cache lifetime (in seconds)</p> <p>Specifies the time to live (TTL) for internal caches in seconds. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.ads.config.encrypted	<p>Encrypted properties</p> <p>Specifies a comma-separated list of encrypted property keys.</p> <p>Valid input</p> <p>List</p>

Key	Description
com.aris.ads.version	<p>Build version</p> <p>This ARIS document storage version is currently installed. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Number</p> <p>Example</p> <p>11.0.1.123456</p>
com.aris.ads.bulk.size	<p>Size of bulk import</p> <p>Maximum number of items that can be pushed to Elasticsearch by a single query. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p>

16.3.5 Add third-party document management system - Basic Auth







You can configure a third-party document management system.

The systems available are Microsoft® SharePoint 2013, Microsoft® SharePoint 2016, and Microsoft® SharePoint 2019. Please contact your local Software AG sales organization (<http://www.softwareag.com>) for other third-party document management systems.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click the arrow next to **Document management system**.
5. Click **General settings**.
6. Click  **Edit**.
7. Enable **Use third-party document management system**.
8. Optional: If you want to use more than one third-party document management system, enable **Support for multiple document management systems**.
9. Click  **Save**.
10. Click  **Add**. The **Add document management system server** dialog opens.
11. Select the authentication scheme. **Basic Auth** and **OAuth** are available. Select **Basic Auth**.
12. Enter the following (page 304):
 - the server ID
 - the display name of the server
 - the type of the third-party document management system. If you want to use Microsoft® SharePoint 2016 or Microsoft® SharePoint 2019, select **TDMS**. If you want to use Microsoft® SharePoint 2013, select **SP2013**.
 - the server URL
 - the user name of the user allowed to access the third-party document management system content

- the password of this user
- the path to the root folder
- the site collection

13. Click **Save**.

You have added a third-party document management system.

If you want to specify more than one third-party document management system, proceed with step 12 of the procedure steps mentioned above.

16.3.6 Add a third-party document management system - OAuth







You can configure a third-party document management system.

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.

Prerequisite

- You have the **Technical configuration administrator** function privilege.
- OAuth is configured in Microsoft® SharePoint 2016 or Microsoft® SharePoint 2019.
- The client ID and the client secret are available.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click the arrow next to **Document management system**.
5. Click **General settings**.
6. Click  **Edit**.
7. Enable **Use third-party document management system**.
8. Optional: If you want to use more than one third-party document management system, enable **Support for multiple document management systems**.
9. Click  **Save**.
10. Click  **Add**. The **Add document management system server** dialog opens.
11. Select the authentication scheme. **Basic Auth** and **OAuth** are available. Select **OAuth**.

As soon as you have selected **OAuth**, **Client ID** and **Client secret** is displayed instead of the fields **User name** and **Password**.

12. Enter the following (page 304):
 - the server ID
 - the display name of the server
 - the type of the third-party document management system
 - the server URL
 - the client ID
 - the client secret
 - the path to the root folder
 - the site collection
13. Click **Save**.

You have added a third-party document management system.

If you want to specify more than one third-party document management system, proceed with step 12 of the procedure steps mentioned above.





16.3.7 Test connection to a third-party document management system

You can test the connection to a third-party document management system.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click the arrow next to the relevant document management system.
5. Click **Connection**.
6. Click  **Test connection**.

A message is displayed, whether or not the connection to a third-party document management system server specified is valid.





16.3.8 Edit document management system


The system available is Microsoft® SharePoint 2013. Please contact your local Software AG sales organization (<http://www.softwareag.com>) for other third-party document management systems.


Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click the arrow next to **Document management system**.
5. Click the arrow next to the relevant document management system.
6. Click a configuration category (page 304).
7. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

8. Adjust your settings.
9. Click  **Save**.

You have customized your document storage configuration.





16.3.9 Delete third-party document management system

The system available is Microsoft® SharePoint 2013. Please contact your local Software AG sales organization (<http://www.softwareag.com>) for other third-party document management systems.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click the arrow next to **Document management system**.
5. Click the arrow next to the relevant document management system.
6. Click **Connection**.
7. Click  **Delete**. The **Confirmation** dialog opens.
8. Click **OK**.

You have deleted a third-party document management system.

16.3.10 Properties for document management systems

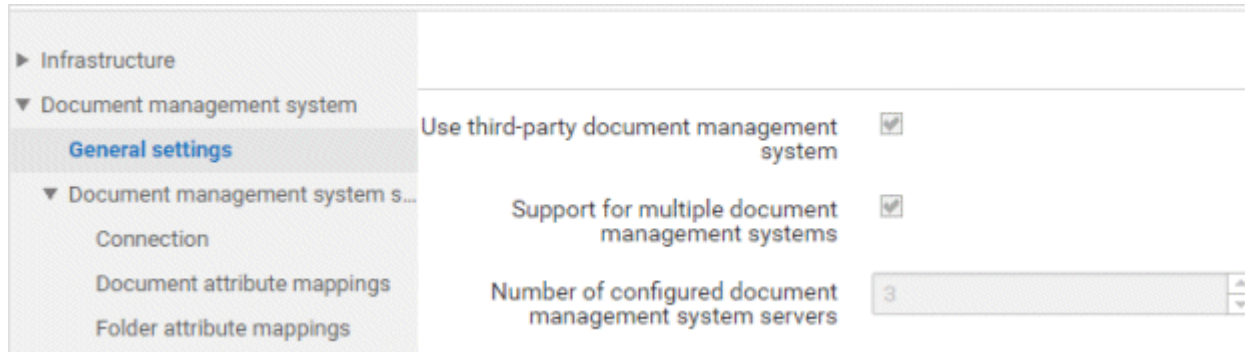
You can configure a third-party document management system (page 302).

The systems available are Microsoft® SharePoint 2013, Microsoft® SharePoint 2016, and Microsoft® SharePoint 2019. Please contact your local Software AG sales organization (<http://www.softwareag.com>) for other third-party document management systems.

GENERAL

Key	Description
com.idsscheer.aris.ads.dms.active	<p>Use third-party document management system</p> <p>Specifies whether or not a third-party document management system can be used. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>

Key	Description
com.idsscheer.aris.ads.dms.multiple.active	<p>Support for multiple document management systems</p> <p>Specifies whether or not more than one third-party document management system can be used. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>
com.idsscheer.aris.ads.dms.configuration.count	<p>Number of configured document management system servers</p> <p>Displays the number of third-party document management systems configured. If you add an additional document management system server, the count is increased by one.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>2</p>



CONNECTION

Key	Description
com.idsscheer.aris.ads.dms.auth.type	<p>Authentication scheme</p> <p>Specifies the type of the authentication scheme.</p>
com.idsscheer.aris.ads.dms.connection.id	<p>ID</p> <p>Specifies the ID of the third-party documents management system.</p> <p>Valid input</p> <p>String</p>
com.idsscheer.aris.ads.dms.display.name	<p>Name</p> <p>Specifies the name of the third-party document management system.</p> <p>Valid input</p> <p>String</p>

Key	Description
com.idsscheer.aris.ads.dms.type	<p>Type</p> <p>Specifies which third-party document management system is to be used, for example, Microsoft® SharePoint 2019.</p> <p>Valid input</p> <p>SP2013, SP2016</p> <p>Example</p> <p>SP2013</p>
com.idsscheer.aris.ads.dms.url	<p>Server URL</p> <p>Specifies the URL of the server on which the third-party document management system is installed.</p> <p>Valid input</p> <p>URL</p>
com.idsscheer.aris.ads.dms.user	<p>User name (Basic Auth)/Client ID (OAuth)</p> <p>Specifies the user name that is granted access to the third-party document management system if Basic Auth is used.</p> <p>Specifies the client ID if OAuth is used.</p> <p>Valid input</p> <p>String</p>

Key	Description
com.idsscheer.aris.ads.dms.password	<p>Password (Basic Auth)/Client secret (OAuth)</p> <p>Specifies the password of the user that is granted access to the third-party document management system if Basic Auth is used.</p> <p>Specifies the client secret if OAuth is used.</p> <p>Valid input</p> <p>String</p>
com.idsscheer.aris.ads.dms.root	<p>Root folder</p> <p>Specifies the name under which access to a third-party document management system is granted.</p> <p>Valid input</p> <p>String</p>
com.idsscheer.aris.ads.dms.site.collection	<p>Site collection</p> <p>Specifies a Microsoft® SharePoint site collection or a subsite containing the document library.</p> <p>Valid input</p> <p>Comma-separated list</p>

- ▶ Infrastructure
- ▼ Document management system
 - General settings
 - ▼ SP1
 - Connection**
 - Document attribute mappings
 - Folder attribute mappings
 - ▶ Quota and restrictions
 - ▶ Search
 - ▶ WebDAV

Authentication scheme	<input type="text" value="Basic Auth"/>
ID	<input type="text" value="SPID1"/>
Name	<input type="text" value="SP1"/>
Type	<input type="text" value="TDMS"/>
Server URL	<input type="text" value="http://myServer"/>
User name	<input type="text" value="jdoe"/>
Password	<input type="password" value="....."/>
Root folder	<input type="text" value="DocLibAds"/>
Site collection	<input type="text"/>

DOCUMENT ATTRIBUTE MAPPINGS

Key	Description
com.idsscheer.aris.ads.dms.document.name	<p>Name</p> <p>Specifies the field to be mapped as the name.</p> <p>Valid input</p> <p>Comma-separated list</p> <p>Example</p>

Key	Description
	FileLeafeRef
com.idsscheer.aris.ads.dms.document.path	Path Specifies the field to be mapped as the path. Valid input String Example FileDirRef
com.idsscheer.aris.ads.dms.document.title	Title Specifies the field to be mapped as the title. Valid input String Example Title
com.idsscheer.aris.ads.dms.document.id	Identifier Specifies the field to be mapped as the identifier. Valid input String Example ID

Key	Description
com.idsscheer.aris.ads.dms.document.size	<p>Size</p> <p>Specifies the field to be mapped as the size.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>FileSizeDisplay</p>
com.idsscheer.aris.ads.dms.document.owner	<p>Owner</p> <p>Specifies a document owner in the third-party document management system.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Owner</p>
com.idsscheer.aris.ads.dms.document.creator	<p>Creator</p> <p>Specifies a document creator for a folder of a third-party document management system.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Author</p>

Key	Description
com.idsscheer.aris.ads.dms.document.created	<p>Created</p> <p>Specifies the field to be mapped as the creation date.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Created</p>
com.idsscheer.aris.ads.dms.document.updated	<p>Updated</p> <p>Specifies the field to be mapped as the creation date.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Modified</p>
com.idsscheer.aris.ads.dms.document.description	<p>Description</p> <p>Specifies the description field for a document in the third-party document management system.</p> <p>Valid input</p> <p>String</p>
com.idsscheer.aris.ads.dms.tags.holder	<p>Tags</p> <p>Specifies a third-party document management system property containing the tags of the document (metadata).</p>

Key	Description
	Valid input Comma-separated list
com.idsscheer.aris.ads.dms.userdefined	Additional fields Comma-separated list of additional fields to be mapped. Valid input Comma-separated list
com.idsscheer.aris.ads.dms.search.fields	Search fields Specifies a comma-separated list of strings that contains the names of the fields used to search for documents in a repository of a third-party document management system. The assistance of an administrator knowing which fields were configured is required. Valid input Comma-separated list Example FileLeafRef, Title

▶ Infrastructure	
▼ Document management system	
General settings	
▼ Document management system s...	
Connection	
Document attribute mappings	
Folder attribute mappings	
▶ Quota and restrictions	
▶ Search	
▶ WebDAV	
	Name <input type="text" value="FileLeafRef"/>
	Path <input type="text" value="FileDirRef"/>
	Title <input type="text" value="Title"/>
	Identifier <input type="text" value="Id"/>
	Size <input type="text" value="FileSizeDisplay"/>
	Owner <input type="text" value="Owner"/>
	Creator <input type="text" value="Author"/>
	Created <input type="text" value="Created"/>
	Updated <input type="text" value="Modified"/>
	Description <input type="text" value="Description0"/>
	Tags <input type="text" value="Keywords"/>
	Additional fields <input type="text"/>
	Search fields <input type="text" value="FileLeafRef,Title"/>

FOLDER ATTRIBUTE MAPPINGS

Key	Description
com.idsscheer.aris.ads.dms.folder.name	<p>Name</p> <p>Specifies the field to be mapped as the name.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>FileLeafeRef</p>
com.idsscheer.aris.ads.dms.folder.path	<p>Path</p> <p>Specifies the field to be mapped as the path.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>FileDirRef</p>

Key	Description
com.idsscheer.aris.ads.dms.folder. id	Identifier Specifies the field to be mapped as the identifier. Valid input String Example ID
com.idsscheer.aris.ads.dms.folder. creator	Creator Specifies a folder creator for a folder of a third-party document management system. Valid input String Example Author
com.idsscheer.aris.ads.dms.folder. created	Created Specifies the field to be mapped as the creation date. Valid input String Example Created

Key	Description
com.idsscheer.aris.ads.dms.folder.updated	<p>Updated</p> <p>Specifies the field to be mapped as the creation date.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Modified</p>
com.idsscheer.aris.ads.dms.folder.userdefined	<p>Additional fields</p> <p>Comma-separated list of additional fields to be mapped.</p> <p>Valid input</p> <p>Comma-separated list</p>

▶ Infrastructure	
▼ Document management system	
General settings	
▼ Document management system s...	
Connection	
Document attribute mappings	
Folder attribute mappings	
▶ Quota and restrictions	
▶ Search	
▶ WebDAV	

Name	<input type="text" value="FileLeafRef"/>
Path	<input type="text" value="FileDirRef"/>
Identifier	<input type="text" value="Id"/>
Creator	<input type="text" value="Author"/>
Created	<input type="text" value="Created"/>
Updated	<input type="text" value="Modified"/>
Additional fields	<input type="text"/>






16.3.11 Customize quota and restrictions

You can configure the quota and restrictions for your document storage.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click **Quota and restrictions**.
5. Click  **Edit**.
6. Adjust your settings.
7. Click  **Save**.

You have configured the quota and restrictions (page 320) for your document storage.

16.3.12 Properties for quota and restrictions

You can configure the quota and restrictions (page 319) for your document storage.

Key	Description
com.aris.ads.config.max.filesize	Maximum file size (in kilobytes) Specifies the maximum allowed size (in kilobytes) for file uploads. Valid input Integer > 0 Example 100
com.aris.ads.config.storage.quota.limit	Quota limit (in kilobytes) Specifies the maximum total size (in kilobytes) of the document storage available to a tenant. Valid input Integer > 0 Example 1000
com.aris.ads.config.storage.quota.usage	Quota usage (in kilobytes) Amount of storage already used (in kilobytes) by uploaded documents. Valid input

Key	Description
	<p>Integer > 0</p> <p>Example</p> <p>9678</p>
com.aris.ads.config.supported.filetypes.filter.active	<p>Restrict file extensions</p> <p>Enables or disables the file extension filter. The default is disabled (default value false).</p>
com.aris.ads.config.supported.filetypes.filter	<p>Valid file extensions</p> <p>Specifies a comma-separated list of allowed file extensions.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>jpeg,jpg,png,gif,pdf,doc,docx,ppt,pptx,pps,ppsx,odt,xls,xlsx</p>
com.aris.ads.config.supported.mimetypes.filter.active	<p>Restrict file types</p> <p>Enables or disables the file type (MIME type) filter. The default is disabled (default value false).</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>
com.aris.ads.config.supported.mimetypes.filter	<p>Allowed file types</p> <p>Specifies the list of allowed file types (MIME types).</p>

Key	Description
	<p data-bbox="629 256 797 288">Valid input</p> <p data-bbox="629 312 719 344">String</p> <p data-bbox="629 376 763 408">Example</p> <p data-bbox="629 432 898 464">text/plain,text/pdf</p>






16.3.13 Configure full-text search


You can display the settings for the full-text search (page 324) in your document storage.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click **Full-text search**.
5. Click  **Edit**.
6. Adjust your settings.
7. Click  **Save**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

16.3.14 Properties for the full-text search

You can display (page 323) the settings for the full-text search in your document storage.

Properties that are highlighted as cross-tenant properties (🔑) can only be changed using ARIS Cloud Controller Command-line Tool (ACC). To change these settings enter the following:

```
reconfigure adsadmin_<size of your installation, s, m, or l> JAVA-D<property name>="<value>"
```

Example

```
reconfigure adsadmin_m JAVA-Dcom.aris.ads.thumbnails.queue.size="40"
```

Key	Description
com.aris.ads.thumbnails.queue.size	<p>Maximum size of thumbnail scaling queue</p> <p>Specifies the maximum size of the queue for creating document thumbnail images. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>50</p>
com.aris.ads.thumbnails.image.size	<p>Maximum size of thumbnail image (in megabytes)</p> <p>Specifies the maximum size of the image used for generating a thumbnail in megabytes.</p>

Key	Description
com.aris.ads.ignoresearch.enabled	<p data-bbox="819 261 1328 292">Exclude marked items from search</p> <p data-bbox="819 319 2002 491">Specifies that a folder or document is to be excluded from the search operation. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual. The default value is false.</p> <p data-bbox="819 518 981 549">Valid input</p> <p data-bbox="819 576 958 606">true, false</p> <p data-bbox="819 638 947 668">Example</p> <p data-bbox="819 695 891 726">False</p>
com.aris.ads.ignoresearch.thread.count	<p data-bbox="819 756 1783 786">Maximum number of threads for items to be excluded from search</p> <p data-bbox="819 813 2033 892">Specifies the maximum number of parallel threads for scaling down items to be excluded from the search operation.</p> <p data-bbox="819 919 981 949">Valid input</p> <p data-bbox="819 976 965 1007">Integer > 0</p> <p data-bbox="819 1038 947 1069">Example</p> <p data-bbox="819 1096 837 1126">3</p>

Key	Description
com.aris.ads.ignoresearch.queue.size	<p>Maximum size of the queue for items to be excluded from search</p> <p>Specifies the maximum size of the queue for folders or documents to be excluded from the search operation.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>50</p>
com.aris.ads.search.restriction.byrole	<p>Enable search restriction</p> <p>Enables or disables whether or not only the last approved version of a document is displayed for users with the ARIS Connect Viewer or ARIS Connect Designer license privilege.</p> <p>Approved means that the document has the metadata status approved. For a user with the ARIS Connect Designer license privilege, two links are displayed additionally, one to open the document and one to display the document details.</p> <p>The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

Key	Description
com.idsscheer.aris.ads.search.elastic.document.maxsize.kb	<p>Maximum document size (in kilobytes)</p> <p>Specifies the maximum document size in Elasticsearch. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>2000</p>
com.idsscheer.aris.ads.search.elastic.parser.memory.threshold.kb	<p>Storage limit (in kilobytes)</p> <p>Specifies the storage limit for the Elasticsearch parser. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>500</p>
com.idsscheer.aris.ads.search.elastic.parser.thread.count	<p>Maximum number of parallel threads</p> <p>Specifies the maximum number of threads for parallel processing when indexing documents. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p>

Key	Description
	<p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>10</p>
com.idsscheer.aris.ads.search.elastic.parser.queue.size	<p>Maximum queue size</p> <p>Specifies the maximum size of the queue for indexing documents. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>10</p>
com.aris.ads.search.term.consolidation.threshold	<p>Threshold for word consolidation</p> <p>Number of recurrent words the application collects before performing an in-memory word consolidation.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>10000</p>

Key	Description
com.aris.ads.search.parser.alwaysembedded	<p data-bbox="817 263 2078 295">Use in-memory parsing for all documents</p> <p data-bbox="817 319 2078 446">Specifies that in-memory parsing is to be used for all documents regardless of their file size. The default value is false. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p data-bbox="817 518 974 550">Valid input</p> <p data-bbox="817 574 963 606">true, false</p> <p data-bbox="817 638 952 670">Example</p> <p data-bbox="817 694 896 726">False</p>






16.3.15 Configure WebDAV


You can display the WebDAV settings (page 331) in your document storage.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Document storage**.
4. Click **WebDAV**.
5. Click  **Edit**.
6. Adjust your settings.
7. Click  **Save**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

16.3.16 WebDAV properties

You can display the WebDAV settings (page 330) in your document storage.

Key	Description
com.softwareag.ads.webdav.repository	<p>Repository</p> <p>Specifies the name of the repository for which WebDAV is to be available. There can only ever be one repository per tenant.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>apg</p>
com.softwareag.ads.webdav.tenant	<p>Tenant</p> <p>Specifies the tenant for which a WebDAV mapping exists. Please note that when you use multiple LDAP servers (page 164), WebDAV works for local users only.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>default</p>

16.4 Configure Process Governance

You can customize general settings of Process Governance.





16.4.1 Import configuration

You can import configurations, which were, for example, exported from a different tenant, into any tenant or installation and use them there. This is an easy way to specify properties that are valid for all tenants on all tenants. This includes, for example, infrastructure settings, publishing settings, or the workflow policies. We recommend that you backup (page 332) your existing configuration before you import a configuration in case that the imported configuration does not meet your expectations.

Prerequisite

- You have the **Process Governance administrator** function privilege.
- You have allowed pop-ups for the pages of ARIS Administration.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Process Governance**.
4. Click  **Import configuration file**.

The **Import configuration file** dialog opens. Navigate to the location where the configuration file is stored and import it. The new configuration is active immediately and no system restart is required.





16.4.2 Export configuration

You can export configurations in order to import them into any tenant or installation and use them there. This is an easy way to specify properties that are valid for all tenants on all tenants.

Prerequisite

- You have the **Process Governance administrator** function privilege.
- You have allowed pop-ups for the pages of ARIS Administration.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Process Governance**.
4. Click  **Export current configuration as a file**.

You can save the configuration file of Process Governance at the relevant location for further use.

16.4.3 Set up sending notifications to Process Governance administrators

You can specify that Process Governance administrators receive e-mail notifications if problems occur during process execution for users modeled in an organizational chart relevant to Process Governance.

Prerequisite

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

Procedure

1. Assign the relevant users Process Governance administrator privileges.
2. Also, specify (page 17) the **E-mail address** attribute for the Process Governance administrators.

The Process Governance administrators will automatically receive an e-mail if problems occur during process execution, for example, if an error occurs during execution of an automated task or if the recipient of an e-mail message has not been entered as a user.






16.4.4 Customize notification settings

You can enable that e-mail notifications are simulated. That means that they are not sent to their recipients.

Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Process Governance**.
4. Click **Notifications**.
5. Click  **Edit**.
6. Adjust you settings (page 340).
7. Click  **Save**.

You have enabled/disabled that e-mail notifications are simulated.






16.4.5 Enable/Disable HTML e-mail notifications

You can enable that e-mail notifications are sent in HTML format.

Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Process Governance**.
4. Click **Notifications**.
5. Click  **Edit**. Click **Enable HTML e-mail** to enable/disable that e-mails are sent in HTML format.
6. Click  **Save**.

You have enabled/disabled HTML e-mail notifications.

16.4.6 Customize HTML templates for e-mail notifications





You can customize the HTML templates for notifications that are automatically sent, for example, for reminder, escalation, or substitution e-mails. You can customize the HTML template in different languages. The templates consist of an HTML and a non-HTML section for these two possible modes. Due to security reasons, JavaScript is not allowed.

Variables (page 335) may be used to personalize the content of a notification. Variables can be used in both notification subject and body.

Prerequisite

- You have the Process Governance administrator (page 110) function privilege.
- You have knowledge in HTML and CSS.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Process Governance**.
4. Click **Notifications**.
5. For the relevant e-mail type, click  **Edit**. You can customize the HTML e-mail templates in the template editor. If you click **Preview**, the customized e-mail is sent to your e-mail address. You find further information about the variables you can use for this specific e-mail type if you click **Help**.
6. Click **Save template**.

You have customized the HTML e-mail template for notifications.

16.4.7 What variables can you use?

Variables may be used to personalize the content of a notification. Variables can be used in both notification subject and body. You can use different variables depending on the e-mail type. The following variables are supported:

- **\$processBoardUrl**
My tasks URL link
- **\$body**
To use text content that has been mapped in the corresponding dataflow in ARIS Architect
- **\$connectLogoUrl**
URL of the ARIS Connect logo
- **\$subject**
Use subject that has been mapped in the corresponding dataflow in ARIS Architect
- **\$serverUrl**
Server URL link
- **\$processName**
Process name
- **\$activityName**
Name of the activity
- **\$tenantName**
Tenant name
- **\$taskAssignee**
User to whom the task was assigned
- **\$taskUrl**
Link to task
- **\$editTaskUrl**
Link to edit task
- **\$dueDate**
Date when the task should be complete
- **\$substitutee**
Target user who acts as the substitute
- **\$originalUserName**

Username of the user who make the substitution

- **\$originalUserDisplayName**

Display name(Last Name,First Name) of the user who make the substitution

- **\$substitutionRole**

Substitution role

- **\$substitutionStartDate**

Substitution start date

- **\$substitutionEndDate**

Substitution end date

16.4.8 Usable tags

You can use the following tags:

- **p** - paragraph
- **div** - used as a container for HTML elements
- **h1, h2, h3, h4, h5, h6** - heading 1 to heading 6
- **ul** - unnumbered list
- **ol** - ordered list
- **li** - list
- **blockquote** - indicates that the enclosed text is an extended quotation
- **b** - bold
- **i** - italic
- **font** - specifies the font face, font size, and color of text
- **s** - strikethrough
- **u** - underlined
- **sup** - superscript
- **sub** - subscript
- **ins** - defines a text that has been inserted into a document. Browsers will usually underline inserted text.
- **del** - defines text that has been deleted from a document. Browsers will usually strike a line through deleted text.
- **strong** - used to define text with strong importance. The content inside is typically displayed in bold.

- **style** - used to define style information (CSS) for a document. Inside the **<style>** element you specify how HTML elements should render in a browser.
- **tt** - was used in HTML 4 to define teletype text
- **code** - defines some text as computer code in a document
- **big** - was used in HTML 4 to define bigger text
- **small** - defines a smaller text
- **br** - inserts a single line break in a text
- **span** - inline container used to mark up a part of a text, or a part of a document
- **em** - emphasis
- **html** - represents the root of an HTML document
- **head** - container for metadata.
- **img** - used to embed an image
- **body** - defines the document body
- **a** - defines a hyperlink
- **table** - defines an HTML table
- **tr** - table row
- **td** - defines a standard data cell in an HTML table
- **rect** - used to create a rectangle and variations of a rectangle shape when using SVG shapes
- **tbody** - used to group the body content in an HTML table
- **thead** - used to group header content in an HTML table
- **pre** - text in a **<pre>** element is displayed in a fixed-width font, and the text preserves both spaces and line breaks. The text will be displayed exactly as written in the HTML source code.
- **meta** - defines metadata about an HTML document
- **th** - defines a header cell in an HTML table
- **hr** - defines a thematic break in an HTML page, for example, a shift of topic

16.4.9 List of allowed attributes inside each tag

Tags	Attributes
a	"href","rel","target"
img	"src"
meta	"http-equiv","content", "charset"
table	"border","cellpadding","cellspacing"
div	"align"
td	"colspan", "valign"
tr	"rowspan"
Allowed in all tags	"id", "class", "style", "type", "height", "width", "class", "align", "title", "name"

16.4.10 Notification properties

You can customize the HTML e-mail templates (page 335).

This is where you find an overview of keys and value pairs:

Key	Description
com.aris.age.email.simulate.only	<p>Simulate notifications</p> <p>Specifies that notifications are not to be sent to their recipients. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

Key	Description
com.aris.age.email.group.by.local e.enabled	<p data-bbox="631 258 2078 295">Grouping of e-mails by language</p> <p data-bbox="631 316 2078 400">Sends a specified message to a user or user group in the preferred language (Locale). The preferred language is specified when a user or user group is created. The default value is false.</p> <p data-bbox="631 421 2078 458">Prerequisites</p> <ul data-bbox="631 478 2078 815" style="list-style-type: none"><li data-bbox="631 478 2078 515">▪ For all constants containing e-mail texts, the texts must be available in all languages.<li data-bbox="631 536 2078 663">▪ The constants must be of the data type Localized string. To use this, you must adjust the data flows. See Model data flows of the ARIS Architect online help (Special topics and functions > Process Governance > Model > Model data flows).<li data-bbox="631 684 2078 815">▪ Re-generate the automated processes and start them. See Generate executable process of the ARIS Architect online help (Special topics and functions > Process Governance > Perform > Generate executable process). <p data-bbox="631 836 2078 873">Valid input</p> <p data-bbox="631 893 2078 930">true, false</p> <p data-bbox="631 951 2078 987">Example</p> <p data-bbox="631 1008 2078 1045">False</p>

Key	Description
com.idsscheer.age.reminder.notification.time	<p>Reminder notification threshold</p> <p>Specifies when a reminder notification is to be sent when X% of the amount of time that is expected to elapse until the due date have already been consumed. The default value is 75 %.</p> <p>Valid input</p> <p>Number > 0</p> <p>Example</p> <p>75</p>
com.idsscheer.age.substitution.notification.enabled	<p>Notify when a substitute is activated</p> <p>Specifies whether or not a notification is sent when a substitute is configured for a task.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

Key	Description
com.aris.age.email.html.enabled	Enable HTML e-mail Enables/disables the sending of e-mails in HTML format. If this option is disabled, e-mails are sent in text format (the synchronization may take a minutes). Valid input true, false Example False
com.aris.age.email.escalation.template	Template for escalation e-mail Template for an escalation e-mail (the synchronization may take a minute).
com.aris.age.email.reminder.template	Template for reminder e-mail Template for a reminder e-mail (the synchronization may take a minute).
com.aris.age.email.substitution.template	Template for substitution e-mail Template for a substitution e-mail (the synchronization may take a minute).
com.aris.age.email.substitution.cancel.template	Template for substitution cancelation e-mail Template for a substitution cancelation e-mail (the synchronization may take a minute).
com.aris.age.email.notification.template	Template for notification e-mail Template for a notification e-mail (the synchronization may take a minute).
com.aris.age.email.assignment.template	Template for assignment e-mail Template for an assignment e-mail (the synchronization may take a minute).

16.4.11 Customize infrastructure settings


You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.


Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Process Governance**.
4. Click **Infrastructure**.
5. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

6. Adjust your settings (page 345).
7. Click  **Save**.

You have customized your system configuration.

16.4.12 Infrastructure properties

You can configure your Process Governance infrastructure (page 344).

Properties that are highlighted as cross-tenant properties can only be changed using ARIS Cloud Controller Command-line Tool. To change the settings, enter the following command:

```
reconfigure apg_<size of your installation, s, m, or l> JAVA-D<property name>="<value>"
```

Example

```
reconfigure apg_m JAVA-Dcom.idsscheer.age.activity.ws.call.timeout="https://myserver.com"
```

This is where you find an overview of keys and value pairs:

Key	Description
com.idsscheer.age.config.encrypted	<p>Encrypted properties</p> <p>Specifies the configuration properties with encrypted values in a comma-separated list.</p> <p>Valid input</p> <p>String</p>
com.idsscheer.age.activity.ws.call.timeout	<p>Web service read timeout</p> <p>Specifies the timeout for read access to a Web service in milliseconds.</p> <p>Valid input</p> <p>Number > 0</p> <p>Example</p> <p>43200000</p>

Key	Description
com.idsscheer.age.xe.maxExecDuration	<p>Maximum execution time</p> <p>Specifies the maximum execution time in milliseconds for activities that support a timeout. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Number > 0</p> <p>Example</p> <p>43200000</p>
com.idsscheer.age.query.maxResults	<p>Maximum query result size</p> <p>Specifies the maximum number of items that are to be returned by a single query. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Number > 0</p>
com.idsscheer.age.log.dblogger.severity	<p>Log level</p> <p>Specifies the log level relevant for logging messages in a log file. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Number > 0</p>

Key	Description
com.idsscheer.age.autodeploy.archive	<p>Archive folder</p> <p>Specifies the location of the folder used for archiving automatically generated processes. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p>
com.idsscheer.age.autodeploy.model	<p>Input folder</p> <p>Specifies the location of the folder used for storing automatically generated processes. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p>
com.idsscheer.age.log.monitoring.output.path	<p>Log file output path</p> <p>Specifies the output path for the system monitoring log files. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Path on a server</p>
com.aris.age.email.fail.instance.on.error	<p>Stop process instance if notification fails</p> <p>Specifies that running a process instance should fail if a notification cannot be successfully sent. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p>

Key	Description
	true
com.idsscheer.age.version	Build number Process Governance build number. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual .
com.idsscheer.age.node.assignment.strategy	Node assignment strategy Indicates the node assignment strategy that is currently active. The default value is TENANT_BASED. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual . Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual . Valid input TENANT_BASED, PROCESS_INSTANCE_BASED Example TENANT_BASED

Key	Description
com.idsscheer.retry.failed.instances.on.restart	<p>Restart failed process instances</p> <p>Specifies that a failed activity of an executable process instance is restarted with the same data if the system is available again. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.idsscheer.age.automatic.node.rebalance	<p>Redistribute process instances using the PROCESS_INSTANCE_BASED node assignment strategy</p> <p>Specifies that process instances are to be automatically redistributed across all active Process Governance nodes every time a new Process Governance node is added to the ARIS environment. The default value is true. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>

Key	Description
com.idsscheer.age.batch.processing.size	<p>Batch processing size</p> <p>Specifies the number of process instances to be processed by the engine. Instances move to QUEUED state if the current processing instances count exceeds the configured value. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual. The default value is 1000.</p> <p>Valid input</p> <p>Integer > 0</p>
com.idsscheer.age.priority.queue.size	<p>Priority queue size</p> <p>Specifies the size of the priority queue. The priority queue contains the instances that are to be run with high priority. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual. The default value is 100.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.age.auditlog.enabled	<p>Generate audit logs</p> <p>Enables the generation of audit logs. Disabling audit logs affects what is displayed in the charts of the 'Governance' category in ARIS Administration. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>

Key	Description
com.aris.age.backup.snapshotBasedBackupMode.enabled	<p>Use snapshot-based backup mode</p> <p>If a tenant backup containing Process Governance data takes a long time to complete, long downtime for Process Governance is likely. To reduce Process Governance downtime while the backup is in process, you can enable the Use snapshot-based backup mode option.</p> <p>This option enables/disables the snapshot-based backup mode for PostgreSQL, Oracle®, and Microsoft® SQL Server databases. You might need to optimize the database settings if you use this option. Please refer to the documentation of the relevant database for more information.</p> <p>If you enable this option, the Multiversion Concurrency Control (MVCC) is used. This is a method from database technology that is used to execute concurrent access to a database as efficiently as possible without blocking or endangering the consistency of the database. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.age.quota.running.instances	<p>Limit of running instances</p> <p>Specifies the number of running instances the tenant is allowed to process.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>100</p>

Key	Description
com.aris.age.quota.queued.instances	<p>Limit of queued instances</p> <p>Specifies the number of queued instances the tenant is allowed to process.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>50</p>
com.aris.age.quota.total.instances	<p>Limit of total instances</p> <p>Specifies the number of total instances the tenant is allowed to process. This includes instances in all states like running, queued, suspended, completed, terminated, and failed.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>150</p>

16.4.13 Customize Publishing


You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.


Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Process Governance**.
4. Click **Publishing**.
5. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

6. Adjust your settings (page 354).
7. Click  **Save**.

You have customized your system configuration.

16.4.14 Publishing properties

You can configure Process Governance Publishing (page 353).

Properties that are highlighted as cross-tenant properties can only be changed using ARIS Cloud Controller Command-line Tool. To change the settings, enter the following command:

```
reconfigure apg_<size of your installation, s, m, or l> JAVA-D<property name>="<value>"
```

Example

```
reconfigure apg_m JAVA-Dcom.idsscheer.age.activity.ws.call.timeout="https://myserver.com"
```

This is where you find an overview of keys and value pairs:

Key	Description
com.idsscheer.age.serviceenabling.staticExport.exportToDisk	<p>Export to server hard drive</p> <p>Specifies that a static export is to be saved on a hard drive of the server. This works only in a non-distributed scenario in which everything is installed on a single server.</p> <p>If this value is set to false, the export is saved as a ZIP file to ARIS document storage and a link is generated. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>
com.idsscheer.age.serviceenabling.staticExport.exportDir	<p>Static export directory</p>

Key	Description
	<p data-bbox="631 256 1234 284">Specifies the directory for the static export.</p> <p data-bbox="631 312 792 339">Valid input</p> <p data-bbox="631 368 1809 395"><Installation directory>/server/bin/work/work_apg_m/base/webapps/aris/apgstatic</p> <p data-bbox="631 432 759 459">Example</p> <p data-bbox="631 488 1644 515">D:/ARIS9.5/server/bin/work/work_apg_m/base/webapps/aris/apgstatic</p>






16.4.15 Customize Reporting

You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.

Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Process Governance**.
4. Click **Reporting**.
5. Click  **Edit**.
6. Adjust your settings (page 357).
7. Click  **Save**.

You have customized your system configuration.

16.4.16 Reporting properties

You can configure Process Governance Reporting (page 356). This is where you find an overview of keys and value pairs:

Key	Description
com.idsscheer.age.serviceenabling.scriptrunner.defaultLanguage	<p>Default method language</p> <p>Specifies the default method language for the ARIS services.</p> <p>Valid input</p> <p>en_US</p> <p>Example</p> <p>en_US, de_DE</p>
com.idsscheer.age.serviceenabling.allowed.document.directory.paths	<p>Allowed document directory paths</p> <p>Restricts the directory paths that are allowed for storing or uploading documents to the server (white list). If no path is specified, all paths are allowed.</p> <p>Valid input</p> <p>Path</p> <p>Example</p> <p>C:\documentpath1,c:\documentpath2,C:\documentpath3</p>






16.4.17 Customize workflow policies

You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.

Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Process Governance**.
4. Click **Workflow policies**.
5. Click  **Edit**.
6. Adjust your settings (page 359).
7. Click  **Save**.

You have customized your system configuration.

16.4.18 Properties for workflow policies

You can configure the workflow policies (page 358) for Process Governance.

Key	Description
com.idsscheer.age.days.workingdays.enabled	Consider only work days Specifies whether only work days are to be considered in an escalation. Valid input true, false
com.idsscheer.age.days.off	Weekend days Specifies which days of the week represent the weekend in a five-day week. The week starts on Sunday (day 1) and ends on Saturday (day 7). Valid input String Example 1,7 Weekends Saturday and Sunday.

Key	Description
com.idsscheer.age.days.publicholidays	<p>Public holidays</p> <p>Specifies the public holidays. The format is DD.MM., for example, 01.01.,24.12.</p> <p>Valid input</p> <p>Date</p> <p>Example</p> <p>01.01,07.01,08.03,...</p>
com.idsscheer.age.e.signature.enabled	<p>E-signature (double authentication)</p> <p>Specifies whether or not reentering the password is necessary when completing tasks. The default value is false.</p> <p>Prerequisites</p> <ul style="list-style-type: none">▪ If not already done, assign a user name and password to the function element fields in the data flow for each automated process in ARIS Architect. See Model data flows of the ARIS Architect online help (Special topics and functions > Process Governance > Model > Model data flows).▪ Re-generate the automated processes and start them. See Generate executable process of the ARIS Architect online help (Special topics and functions > Process Governance > Perform > Generate executable process). <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

Key	Description
com.idsscheer.age.e.signature.us ername.enabled	<p data-bbox="631 258 2078 300">Enable user name field in e-signature (double authentication)</p> <p data-bbox="631 306 2078 450">Enables/Disables user name protection for human tasks. User name protection is enabled only if both this option and the E-signature (double authentication) option are selected. The default value is false. If SSO is used, users must enter the password only.</p> <p data-bbox="631 466 2078 507">Prerequisites</p> <ul data-bbox="631 513 2078 801" style="list-style-type: none"><li data-bbox="631 513 2078 657">▪ If not already done, assign a user name and password to the function element fields in the data flow for each automated process in ARIS Architect. See Model data flows of the ARIS Architect online help (Special topics and functions > Process Governance > Model > Model data flows).<li data-bbox="631 663 2078 801">▪ Re-generate the automated processes and start them. See Generate executable process of the ARIS Architect online help (Special topics and functions > Process Governance > Perform > Generate executable process). <p data-bbox="631 817 2078 858">Valid input</p> <p data-bbox="631 865 2078 906">true, false</p> <p data-bbox="631 912 2078 954">Example</p> <p data-bbox="631 960 2078 1002">False</p>

Key	Description
com.idsscheer.age.taskList.delegation.enabled	<p>Allow task delegation</p> <p>Specifies whether or not delegation of tasks to other users (Delegate/Substitution) is allowed.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>
com.idsscheer.age.taskList.startTaskConfirmation.enabled	<p>Confirm start of task execution</p> <p>Specifies centrally for all users whether or not the confirmation dialog is displayed when a task is started for the first time.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>

16.4.19 Customize pools


You can customize your system configuration as required. You carry out this part of the configuration in ARIS Administration.


Prerequisite

You have the Process Governance administrator (page 110) function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Process Governance**.
4. Click **Pools**.
5. Click  **Edit**.

The **Cross-tenant** symbol  indicates that the settings made apply to all tenants on this server and cannot be changed.

6. Adjust your settings (page 364).
7. Click  **Save**.

You have customized your system configuration.

16.4.20 Properties for pools

You can configure thread pools (page 363) for Process Governance.

Properties that are highlighted as cross-tenant properties can only be changed using ARIS Cloud Controller Command-line Tool. To change the settings, enter the following command:

```
reconfigure apg_<size of your installation, s, m, or l> JAVA-D<property name>="<value>"
```

Example

```
reconfigure apg_m JAVA-Dcom.idsscheer.age.activity.ws.call.timeout="https://myserver.com"
```

This is where you find an overview of keys and value pairs:

Key	Description
com.idsscheer.age.job.service.threadsNumber	<p>Pool size of job service threads</p> <p>Specifies the number of threads to be used by the job service. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual. The default value is 8.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>8</p>

Key	Description
com.idsscheer.age.simulation.instanceExecutorsPool.size	<p>Simulation pool size</p> <p>Specifies the size of the pool containing simulated process instances. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual. The default value is 5.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>5</p>
com.idsscheer.age.xe.dispatch.workersPool.size	<p>Pool size of dispatch worker threads</p> <p>Specifies the pool size for dispatch worker threads. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual. The default value is 10.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>10</p>

Key	Description
com.idsscheer.age.xe.webservice.jobs.pool.size	<p>Pool size of web service worker threads</p> <p>Specifies the pool size for web service worker threads. The default value is 15. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>15</p>
com.idsscheer.age.webservice.abs.connections.pool.size.per.node	<p>Maximum number of connections allowed for a single node</p> <p>Specifies the maximum number of connections that can be created in the connection pool of the http client for one ARIS Server node. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>10</p>

Key	Description
com.idsscheer.age.webservice.abs.connections.pool.size	<p>Total number of connections allowed in connections pool</p> <p>Specifies the maximum number of connections that can be created in the connection pool of the http client for all <_a_serverI> nodes. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>100</p>

16.5 Configure Collaboration

You can customize general settings of Collaboration.





16.5.1 Customize Collaboration

You can customize Collaboration.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Collaboration**.
4. Click a configuration category (page 370).
5. Click  **Edit property** in the row of the property you want to configure.

If Collaboration is deactivated, the properties are also deactivated and cannot be edited.

You have configured Collaboration.





16.5.2 Refresh list of published databases

You can refresh the list of published databases.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Collaboration**. If Collaboration is deactivated, the properties are also deactivated and cannot be edited.
4. Click **Configure database**.
5. Click  **Refresh database list**.

You have refreshed the list of published databases.

16.5.3 Manually synchronize database





If a user name is set for the **Person responsible** model attribute of a model in an ARIS database, this user automatically becomes a follower of this model. Once the automatic following is activated in Collaboration), this user can see all model activities in **My feed**, and receives notifications about them. However, this only applies if this user has at least the **Read (r---)** access privilege in the corresponding ARIS database.

You can synchronize a database manually at any time.

Prerequisite

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

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Collaboration**. If Collaboration is deactivated, the properties are also deactivated and cannot be edited.
4. Click **Configure database**.
5. Move the mouse cursor in the row of the database you want to synchronize.
6. Click  **Refresh database list**.

You have refreshed the content of a database for Collaboration.

16.5.4 Properties for Collaboration

The following can be customized in Collaboration.

GENERAL SETTINGS

Key	Description
collaboration.optionsPage.enableECP	Activate Collaboration Activates Collaboration. The default value is true . Valid input true, false Example true
collaboration.optionsPage.allowCreationOfGroups	Create groups Specifies whether or not creating groups in Collaboration is allowed. The default value is true . Valid input true, false Example true

Key	Description
collaboration.optionsPage.allowCreationOfFilters	<p>Create filters</p> <p>Specifies whether or not creating filters in Collaboration is allowed. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>
collaboration.optionsPage.enableLikeButton	<p>Enable Like button</p> <p>Specifies whether or not the Like button is displayed. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>
collaboration.optionsPage.allowCommenting	<p>Create comments</p> <p>Specifies whether or not comments on content are allowed. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>

Key	Description
collaboration.optionsPage.allowSharing	<p>Share content</p> <p>Specifies whether or not sharing of content is allowed. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>
collaboration.optionsPage.allowBookmarks	<p>Create bookmarks</p> <p>Specifies whether or not creating bookmarks is allowed. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>
collaboration.optionsPage.allowTags	<p>Create tags</p> <p>Specifies whether or not creating tags is allowed. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>

Key	Description
collaboration.optionsPage.allowFlags	<p>Flag activities</p> <p>Specifies whether or not flagging content is allowed. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>
collaboration.optionsPage.allowTagFilterInMainStream	<p>Allow tag filtering (My feed)</p> <p>Specifies whether or not filtering using tags is allowed on the Collaboration start page. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>

Key	Description
collaboration.optionsPage.allowTagFilterInFullStream	<p>Allow tag filtering (Portal)</p> <p>Specifies whether or not filtering using tags is allowed in the My activities area. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>
collaboration.optionsPage.allowTagFilterInCommentStream	<p>Allow tag filtering (My portal feeds)</p> <p>Specifies whether or not filtering using tags is allowed in the portal. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>

Key	Description
collaboration.optionsPage.filterPrivateFeeds	<p>Public access to portal feeds</p> <p>Specifies whether posts to model feeds are visible only if a user is following the model feed or is a member of a group that is following the model feed. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>
collaboration.optionsPage.tagsClosedSearchOperator	<p>Search operator 'OR' instead of 'AND'</p> <p>If this parameter is set to 'true', search operator 'OR' is used for tags in ARIS Connect instead of 'AND'. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>

Key	Description
collaboration.optionsPage.enableAttachment	<p>Enable attachments</p> <p>Specifies whether or not documents from ARIS document storage can be accessed as new attachments for activities. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>true</p>
collaboration.optionsPage.exportActivitiesAsZipFileInstantly	<p>Export activities as a ZIP file instantly</p> <p>Specifies whether activities are exported as a ZIP file instantly or whether the ZIP file will be stored in ARIS document storage and you can download it later. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>

Key	Description
collaboration.optionsPage.autoFollowGroup	<p>Automatically follow groups</p> <p>Specifies whether or not users are automatically followers of groups they have posted to or whose content they have commented on. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>
collaboration.optionsPage.autoFollowUser	<p>Automatically follow users</p> <p>Specifies whether or not users are automatically followers of users they have posted to or whose content they have commented on. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>

Key	Description
collaboration.optionsPage.autoFollowModel	<p>Automatically follow models</p> <p>Specifies whether or not users are automatically followers of models they have posted to or whose content they have commented on. The default value is false.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>
collaboration.optionsPage.minimumSearchTermsCharacters	<p>Minimum length of the search term</p> <p>Specifies the minimum number of characters required to trigger the search in Collaboration. The default value is 3.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>3</p>

CONFIGURE USER GROUP

Key	Description	Valid input	Example
enableAllUserGroups	<p>Enable all user groups</p> <p>Enables the function based on which all ARIS user groups are displayed when users are posting in Collaboration. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>	true, false	false
userGroupsToHaveOwnFeedInCollaboration	<p>Enable the use of user groups in Collaboration user groups</p> <p>Enables that instead of inviting each user individually to join a group in Collaboration, all users of the group enabled are automatically invited when creating this group in Collaboration. The default value is true.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>false</p>	true, false	false

CONFIGURE DATABASE

Key	Description	Valid input	Example
Database	<p>Synchronize daily at</p> <p>Enables that the database is synchronized at a certain time every day if Automatically follow users/Automatically follow groups/Automatically follow models is enabled.</p> <p>If a user name is set for the Person responsible model attribute of a model in an ARIS database, this user automatically becomes a follower of this model. Once the automatic following is activated in Collaboration), this user can see all model activities in My feed, and receives notifications about them. However, this only applies if this user has at least the Read (r---) access privilege in the corresponding ARIS database.</p> <p>If a different user name is set for the Person responsible model attribute at a later point in time, the automatic following remains activated for the previous user until this user manually stops following this model (Unfollow).</p> <p>Valid input</p> <p>Time</p>	time	

17 Manage server tasks



Centrally check server tasks, such as reports, merge operations, or backups. You can cancel report executions. This might be necessary, for example, if incorrect reports are executed.




17.1 Display server tasks

You can check which server tasks, such as reports, merge operations, or backups, are performed and which server tasks are completed.

Prerequisite

You have the **ARIS Connect administrator** and **Server administrator** function privileges.

Procedure

1. Click  **Application launcher** >  **Administration**.
2. Click  **Server tasks**.
3. Click **Running tasks** or **Completed tasks**.

Running tasks or completed tasks are listed.





17.2 Toggle auto-refresh

You can switch auto-refresh on or off. If you have enabled auto-refresh, new tasks are displayed immediately after they are created.

Prerequisite

You must have the **ARIS Connect administrator** and **Server administrator** function privileges to view **server tasks**.

Procedure

1. Click  **Server tasks**.
2. Click  **Toggle auto-refresh** to enable auto-refresh. The icon is underlined to indicate that auto-refresh is enabled and new tasks are displayed immediately after they are created.
3. Click  **Toggle auto-refresh** again if you want to disable auto-refresh. The icon is no longer underlined. To view new tasks from now on, click  **Refresh**.

You have defined whether the tasks are updated automatically or manually.

17.3 Cancel report

You can cancel the execution of a task of the **Report** category, that is, the execution of running reports.



Prerequisite

You must have the **ARIS Connect administrator** and **Server administrator** function privileges to view **server tasks**.

Warning

Canceling a report execution "kills" the report, that is, canceling a report does not guarantee data consistency. If, for example, a report has changed data, these changes are not rolled back by the cancelation.

Procedure

1. Click  **Server tasks**. The tasks currently running are listed.
2. From the user column, determine the name of the user who started the report. Inform the user that the report is to be canceled and he must press **F5** to continue working in ARIS Connect when the cancel dialog opens. This closes the cancel dialog and work in the program is possible again.
3. In the row of the report you want to cancel, click  **Cancel**. The confirmation dialog opens.
4. Click **Yes**.

The report is canceled and displayed in **Completed tasks** with the status **Canceled**. The user who started the report is informed of the cancelation by a cancelation dialog.

17.4 Good to know

This section provides background information to assist you in carrying out the relevant procedures.

17.4.1 What is the Server tasks area for?

The **Server tasks** area lists current and completed server tasks, such as reports, merge operations, or backups, of a tenant. You can see which tasks are running in the background of the tenant and which tasks have been completed and no longer consume resources.

You can use the **Running tasks** list to cancel a task (page 382) of the category **Report**. Canceled tasks are listed in the **Completed tasks** list with the status **Canceled**.

The **Completed task** list displays a maximum of 1.000 tasks. When more tasks are completed, the oldest tasks are removed from the list. Entries older than seven days are automatically removed from the list.

17.4.2 How is the Running tasks list structured?

The **Running tasks** list has the following columns. You can sort the columns in the table in ascending and descending order.

Column	Content
Category	Outputs the category of the server task, such as XML Import , DB Restore , Merge and Report .
Name	Name of the task.
User	Name of the user who started the task.
State	Status of the task, for example, Initializing and Running . Depending on the category of the task, additional information is provided, for example, The request is in the processing queue for reports.
Server	Server on which the task is executed.
Start time	Month, day, and time at which the task was started.
Duration	Duration of the task in milliseconds, seconds, minutes, etc.

17.4.3 How is the Completed tasks list structured?

The **Completed tasks** list has the following columns. You can sort the columns in the table in ascending and descending order.

Column	Content
Category	Outputs the category of the server task, such as XML Import , DB Restore , Merge and Report .
Name	Name of the task.
User	Name of the user who started the task.
State	Status of the task, for example, Completed or Canceled .
Server	Server on which the task was executed.
Start time	Month, day, and time at which the task was started.
Duration	Duration of the task in milliseconds, seconds, minutes, etc.

18 Make default dashboards available

This procedure explains how to provide default ARIS Aware dashboards in ARIS Connect. For demonstration purposes, you can display demo dashboards. These dashboards are available in the **United Motor Group** demo database.

Prerequisites

- Your ARIS Server is enabled for ARIS Aware that is, the **dashboarding** runnable is activated and running (see **ARIS Server Installation Guide** or **ARIS Cloud Controller (ACC) Command-Line Tool** on DVD 3, ARIS Download Center (<https://aris.softwareag.com/>), or Empower (<https://empower.softwareag.com/>)).
- A valid **ARIS Connect Server Extension Pack Aware (YCSAW)** license is available in ARIS Administration > User Management.
- Users either need an **ARIS Connect Viewer** license + **ARIS Connect Viewer Extension Pack Aware User (YCSCA)** license to see dashboards or an **ARIS Connect Designer Extension Pack Aware User (YCSDA)** license to modify dashboards.
- You have access to the ARIS installation DVD 3.
- If you want use Matomo to generate dashboards based on portal usage statistics of ARIS Connect content, additional prerequisites must be met (page 397).

Procedure

1. Import the default XML documents. You can either do a bulk import using a command line tool (page 386) (for initial installation only) or copy the documents using WebDAV (page 387).

These documents are used by the default data feeds. This imported static content is used to generate demo dashboards.

If you use default dashboards to display own productive data, you must update the xml documents regularly by scheduled reports (see step 6). These reports are used to create and update input data used by the default data feeds to generate default dashboards. When reports update XML documents, demo dashboards are no longer provided properly because the fictive data used to generate the demo dashboards is overwritten.

Warning

Do not import default xml documents to an updated ARIS installation. Otherwise current data will be overwritten by static demo data and dashboards will no longer display your data.

2. Import default dashboard content (page 389).
3. Add an alias URL (page 390).
4. Check default data feeds for issues (page 391).

5. Publish the database as a process portal (page 139, page 427) using the **default** or **classic** configuration set. After the XML documents were updated by the related reports, dashboards using **Center of Excellence (CoE)** data are only available if the portal is based on the **default** configuration set or a related modification set.
6. Keep dashboard data up to date (page 394).
7. Create (page 36) a new **dashboard_viewers** user group in ARIS Administration and assign all users which should see dashboards but are no Dashboard administrators. Otherwise, you must assign permissions for all dashboards and the corresponding feeds separately to every user in the data feed editor.

All default dashboards, data feeds and documents are available in ARIS Connect.

18.1 Bulk Import using Command Line Tool

INITIAL INSTALLATION

For new installations, you can import documents using the Command line tool. These documents are used by the default data feeds to generate dashboards.

Procedure

1. Extract the **Documents** archive (ARIS installation DVD 3\Content\ARISAware) to a temporary target directory, for example: **C:\Dashboarding**. This archive contains all required XML documents used by the default data feeds.
2. Import the default ARIS document storage documents via bulk import:
3. Open a Command Prompt and navigate to <ARIS installation path>\server\bin\work\work_adsadmin_<s, m, or l>\tools\bin.
4. Enter this command to import all documents into ARIS document storage of each tenant you use, for example, **default**:

```
y-admintool.bat -t <tenant name> bulkimport -u system -p manager -path "c:\Dashboarding"
```

c:\Dashboarding is the extracted structure from zip archive and location on the server storage.

5. Check for the shown message of 162 imported files in 10 folders for each tenant.
6. Close the Command Prompt window.

All default XML documents are available in ARIS document storage.

You must import the default data feeds (page 389) to generate default dashboards.

UPDATE INSTALLATION

Do not use the bulk import command line tool in case of an update installation.




Upload the **Conversation_Rate.csv** document manually to the **Dashboarding** folder.

Upload the following files manually to the **Dashboarding\<database name>\CXM** folder, for example, **Dashboarding\United Motor Group\CXM**, of each database:

- CXM_SEGMENTATION_AND_ASSIGNMENTS.xml
- CXM_SEGMENTATION_AND_ASSIGNMENTS_METADATA.xml

You can find these files in the **Content\ARISAware\Documents.zip** file from the ARIS installation DVD 3.

Procedure

1. Open ARIS Connect.
2. Click  **Application launcher** >  **Models & Objects**.
3. Click **Documents**.
4. Click a folder in the navigation.
5. Click  **Upload**. The **Upload document** (page 101) dialog opens.
6. Enter the relevant optional additional information and click **OK**.

You have added a new content for ARIS Aware.

18.2 Copy documents using WebDAV

You can import the default ARIS document storage documents using WebDAV. These documents are used by the default data feeds to generate dashboards.

ARIS document storage supports WebDAV. You can connect only one tenant with a specific repository.

To grant users without the **Document management** role access to ARIS document storage content, ARIS document storage can be used as a WebDAV network drive.

With a Microsoft® Windows 7 operating system you just need to connect the relevant network and access ARIS document storage directly. With older operating systems, you need to use Web folders (select **Tools > Map Network Drive > Sign up for online storage connect to a network server** in Microsoft® Windows Explorer). If this does not work, you must configure your computer as follows.

Procedure

1. Open the Registry Editor.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters** and find the DWORD entry **BasicAuthLevel**.
3. Check if the value of this entry is **2**. If the value of this entry differs, please change it to **2**. If the DWORD entry does not exist, create it.
4. With operating systems older than Microsoft® Windows 7 you also need to find the DWORD entry **UseBasicAuth**. If it does not exist, create it.
5. Change the value of this entry to the hexadecimal value **1**. Thus, you enable HTTP Basic Access Authentication for SSL and non-SSL connections.
6. Close the Registry Editor.
7. Restart Microsoft® Windows.

You can now use ARIS document storage as a WebDAV network drive.

8. Configure ARIS document storage for WebDAV - please refer to the ARIS Connect online help, chapter **Manage ARIS Connect > Configure ARIS Connect > Set up Document storage > Configure WebDAV**.
9. Extract the **Documents** archive (ARIS installation DVD 3\Content\ARISAware) to a temporary target directory, for example: **C:\Dashboarding**. This archive contains all required XML documents used by the default data feeds.
10. To copy the content into ARIS document storage, a network mapping using WebDAV is required.

11. Map the network drive to **http://<Fully qualified domain name of ARIS Server:load balancer port>/documents/rest/webdav**. You do not need to specify the port if the load balancer uses port 80.

Example

http://myserver.mydomain.ext:1081>/documents/rest/webdav

12. Copy extracted folder **Dashboarding** to mapped network drive.

All default documents are available in ARIS document storage.

You must import the default data feeds (page 389) to generate default dashboards.





18.3 Import default dashboard content

The default dashboards and data feeds must be imported. These default data feeds are configured to use the corresponding XML documents. Therefore, make sure you have imported the required XML documents (see bulk import (page 386) or using WebDAV (page 387)).

Prerequisite

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

Procedure

1. Copy the **Dashboards_Feeds.zip** file from the ARIS installation DVD 3 (..\Content\ARISAware) to a temporary target directory, for example to: **C:\Dashboarding**. The **Dashboards_Feeds.zip** file contains the default dashboards, data feeds, and permissions.
2. Start ARIS Connect.
3. Click  **Application launcher** >  **Models & Objects**.
4. Activate the **Dashboards & Data feeds** tab.
5. Click  **Dashboards**.
6. Click  **Import**.
7. Import the **Dashboards_Feeds.zip** file. The file contains the default dashboards and dashboard privileges.
8. If the dashboard(s) available in the repository should be replaced, activate the **Overwrite if already exists** option.
9. If the dashboard permissions contained in the dashboard file should also be imported, activate the **Import privileges** option. This option is activated by default.

10. Click **Import**. The default dashboards, data feeds, and permissions are imported, and the new dashboards are listed on the **Dashboards** tab of the repository.

All default dashboards and data feeds are available.

18.4 Add a URL alias for dashboards

Define the alias URL to be used within data feeds. If you specify **Feed URL**, all default data feeds will work properly.





Defining a URL alias enables you to shorten the link used in dashboards and data feeds. If you use an alias, you only specify the path to the location where the data is stored. You do not need to enter the entire URL. Furthermore, adapting the alias enables you to import this kind of data to a different server.

If you have updated ARIS Connect 10.0 Service Release 1 to version 10.0 Service Release 2, you need to recreate the URL alias that WAS defined for ARIS Connect 10.0 Service Release 1. Delete the URL alias at first and add a new URL alias (page 390) with the same data.


Prerequisite

- You have the **Dashboard administrator** function privilege.
- You have an ARIS Connect Designer (page 48) license.
- Your ARIS Server is enabled for ARIS Aware.

Procedure

1. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
2. Click  **Configuration**.
3. Click **Dashboards**.
4. Click **Connections**.
5. Select **URL_ALIAS** from the list.
6. Click  **Add**. The **Add property** dialog opens.
7. Enter the alias. Enter **Feed URL** for the content that is delivered with the installation.
8. Enter the protocol (http or https) to be used for the communication.
9. Enter a fully-qualified host name (FQHN). Enter, for example, **myserver.mydomain.ext**, where ARIS Server runs. You can copy it from your browser's URL.
10. Enter the port on which ARIS Server runs.
11. Enable **Use single sign-on** if you want allow that data sources can be accessed without an additional login. You change this preset option in the data source operator.

12. Enter user name and password of the user who is supposed to have access to the data feeds used by the dashboards.

If you change the password of the user who created this URL_ALIAS, you must also update the password for the **Feed URL** alias ( **Edit Property**), otherwise dashboards cannot be displayed.


13. Click  **Save**.

The alias URL is defined.

This alias URL can be used for your data feeds.

18.5 Check default data feeds for issues




You can open an available data feed in ARIS Connect. The data feed is opened in the data feed editor.

The available dashboards and the relevant data feeds are provided in the  **Repository** of ARIS Connect.

Prerequisite

- You have the **Dashboard administrator** function privilege.
- You have an ARIS Connect Designer (page 48) license.
- The **Feed URL** alias URL is defined (page 390).
- The default ARIS Aware dashboards are available (page 385).


Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Models & Objects**.
3. Activate the **Dashboards & Data feeds** tab.
4. Click  **Data feeds**. The default data feeds are displayed.
5. Click a data feed name.

The selected data feed opens in the data feed editor. The data feed will work properly if the **Feed URL** is in use. If the **Path prefix (alias)** name is shown in red, the alias URL has not been created (page 390) properly.

6. Click  **Calculate preview**.

If data is shown in the **Calculation result of operator ARIS Table** section, the default data feeds work properly. All default dashboards can be displayed in ARIS Connect.

In case of errors check whether the prerequisites specified are met. If you change the password of the user who created this URL_ALIAS, you must also update the password for the **Feed URL** alias ( **Edit Property**), otherwise dashboards cannot be displayed.

18.6 Publish databases




Publish the databases you want to make available under **Published content**. There, users with a **Viewer** or **Designer** license can access the fact sheets of the models and objects of the databases.

To start executables and download SAP documents, or to have the ARIS Online Guide available, you must import (page 424) SAP-related configuration sets for the portal and publish the database in **Published content** (page 139, page 427).

Prerequisite


- You have the **Database administrator** function privilege.
- You have the **Publishing administrator** function privilege.

Procedure

1. Click  **Application launcher** >  **Administration**.
2. Click **Portal** > **Publish databases** if it is not already selected. The  **Configuration** tab displays the **Publish databases** area. All available databases are displayed.
3. Enable the check boxes of the databases you want to publish in **Published content**.
4. For versioned databases, select the relevant version.
5. Click **Apply**.

The content of the databases is published in **Published content** in the selected configuration or modification set. If databases are available in **Published content** they cannot be deleted in ARIS.

18.7 Specify report parameters in ARIS Architect

To generate data feed input for default ARIS Aware Dashboards, the reports listed in the **Dashboard data** category (**Administration** tab >  **Evaluations > Reports**) are available in ARIS Architect.

For some reports, parameters can be specified. These parameterized reports are to be started frequently using report schedules (page 394). This keeps the dashboards up to date. The scheduled reports themselves trigger related reports. Each report collects specific pieces of information. The results are stored in ARIS document storage as XML report output files. These pieces of information are formed into dashboards. That is why dashboards correlate very closely to the set of executed reports.





To use the Matomo - Global portal usage (page 408) and Matomo - Database-specific portal usage (page 407) reports, make sure to have Matomo installed and configured (page 397) and the report parameters specified accordingly (page 405).

All default ARIS Aware Dashboards work together with the **United Motor Group** demonstration ARIS database. Some reports already use default parameters, such as file names and titles of the report results, stored in ARIS document storage. You can change these names and titles in different parameter value sets. If you assign different sets to different databases, the same report can be run on different databases using different parameters.

Prerequisite

You are script administrator for this tenant.

Procedure

1. Start ARIS Architect.
2. In ARIS Architect, click **ARIS >**  **Administration**.
3. Click  **Navigation** in the bar panel if the **Navigation** bar is not activated yet.
4. In the navigation tree, click the folder  **Evaluations > Reports**.
5. Click the **Dashboard data** category (subfolder).
6. Select the report to be made available in ARIS Connect.
7. In the **Start** tab bar, click  **Edit report parameters**. The report parameters are displayed.

On the **Output** tab, for all reports generating input for data feeds, file names, document titles and the ARIS document storage paths are specified. For other reports, such as CoE reports, various other tabs are available, for example, **General**, **Conventions** or **Thresholds**. These tabs categorize parameters defining item types to be evaluated in the defined ways.

If you modify values, the demo system will be affected. You can add **+** and modify duplicated **■** value pairs instead. Click **Assign modification** **■** to apply the changes when executing the report for a specific database.

8. Click **OK**.

The report evaluates data and uses the required parameters.

Users can start parameterized reports using the Report Wizard. If several parameter value sets are defined, the required set can be selected.

18.8 Keep ARIS Aware dashboards up to date





This procedure describes how to define scheduled reports in ARIS Architect.

Database information to be compiled for the dashboard display is gathered by different reports. These reports generate data feed (page 391) input stored in ARIS document storage. Run these reports automatically to keep all data compiled for dashboard display up to date. To use the Matomo - Global portal usage (page 408) and Matomo - Database-specific portal usage (page 407) reports, make sure to have Matomo installed and configured (page 397) and the report parameters specified accordingly (page 405).

Prerequisite

- You have the **Report automation** function privilege for the related database.
- You have access to this script. Access to scripts can be restricted to certain user groups.
- You have read access to all required database groups.

Procedure

1. Start ARIS Architect.
2. Click **ARIS > Administration** or **ARIS > Explorer**. The **Administration** or **Explorer** tab opens.
3. Log in to the database.
4. Click  **Navigation** in the bar panel if the **Navigation** bar is not activated yet.
5. In the Explorer tree, click the folder  **Scheduled reports**.
6. Click  **New >**  **Create scheduled report**. The **Report Automation Wizard** opens.
7. Specify the name for this schedule and enter the user's password that has **read** permission to all required database groups. Make sure that the schedule is activated.
8. Click **Next** and select the required report from the **Dashboard data** category and specify the settings as required.
9. Click **Next** and select the database to be evaluated.
10. Click **Next** and specify the schedule settings as required.
11. Click **Finish**. If the first execution is in the future, the report is automatically active and runs as soon as the defined point in time is reached.
12. Create schedules for all required reports from the **Dashboard data** category. The selection of reports depends on the data to be compiled for dashboard display.

All default data feeds used to create dashboards will be supplied with the most current data as specified.





18.9 Create user group

Create a new user group. User groups define the tasks or functions that a person performs in a company. A certain set of function, license, and database privileges, as well as profiles, is assigned to different user groups. If a user group is assigned to a user, the user has all privileges and profiles assigned to that user group. A user can belong to several different user groups at the same time.

Prerequisite

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

Procedure

1. Open ARIS Administration.
 - a. Click the link that was provided to you by e-mail or that you have saved as a bookmark in your browser. The **Login** dialog opens.
 - b. Enter your user name and your password.
 - c. Click **Log in**.
 - d. Click  **Application launcher** >  **Administration**.
ARIS Administration opens.
2. Click  **User management** and select **User groups**. The list of user groups opens.
3. Click  **Add user group**.
4. Enter the name of the user group and an optional description. If a user group that already exists in the LDAP system is created, the user group names must match. This is the only way to assign an existing ARIS user group with the LDAP user group.
5. Click **Save**.

The user group is created.

If required, product-specific groups must additionally be created and assigned in each ARIS product.

Tip

To transfer user and privilege assignments of a group to a new group, go to the overview of groups and click **Copy group** in the row of the relevant group. Enable the check box of assignments to be transferred and add the remaining data, such as group name, etc. of the new group.

18.10 Using Matomo

If you want to generate dashboards based on portal usage statistics of ARIS Connect content, you must set up and configure the external web analytics application **Matomo** (page 397), install and configure two additional ARIS runnables (page 398), and configure the Matomo-related reports in ARIS Architect (page 405).

ARIS sends portal usage statistics data to Matomo only if users allow tracking. They must disable the **Do not track** browser option.

18.10.1 Set up and configure Matomo

If you want to generate auditing-based dashboards from ARIS Connect content, you must set up and configure the external web analytics application Matomo. Matomo is not included in this ARIS package.

The following describes the Matomo usage in a distributed environment. You can also install Matomo on an existing ARIS server. In this case, ARIS Agent is already installed, and you must only add the additional runnables to the ARIS server. Note that running ARIS and Matomo on one and the same server may result in a considerable loss of performance.

Procedure

1. Set up Matomo.

You must install a Web server, PHP, a database, and deploy the Matomo web application. For further information, refer to the Matomo installation guide.

2. During the Matomo setup, add the website:

Name =ARIS Connect, URL = http://<host>:<port>.

Alternatively, register **ARIS Connect** as a website in an existing Matomo installation.

3. After Matomo is set up, open the its configuration.

4. Enable unique visitors processing for **day**, **week**, **month**, and **range**. Day, week, and month are enabled by default.

5. Because ARIS relies on Matomo segments to behave as a filter, you must disable the segments cache for Matomo versions **3.12.0** and higher.

6. Log in to Matomo.

7. Create a user with **view** permission on the **ARIS Connect** website and copy its authentication token to a text file.

You need the token to parameterize the Matomo reports (page 405) later in ARIS Architect and to configure the **eventsubscriber** runnable (page 398).

8. Install the **Custom Dimensions** Matomo plugin.
9. Activate the plugin.
10. Create a new Custom Dimension named **tenant** for visits and two Custom Dimensions named **resource-path** and **resource-type** for visit actions. Set all of them to active and copy the IDs to the text file. You need the IDs to parameterize the Matomo reports (page 405) later in ARIS Architect and to configure the **eventsubscriber** runnable (page 398).
11. Make sure that site search tracking is enabled for the **ARIS Connect** website.
12. If the ARIS Connect Portal usage is expected to be high, we recommend disabling archiving of browser-triggered Matomo reports. To prevent performance issues, you are recommended to set up auto-archiving as a background task that runs in a fixed interval. You must complete this task before running any scheduled ARIS reports that access the Matomo data.

Matomo is installed and configured to use ARIS.

Install ARIS Agent to the machine where Matomo is running and add the additional runnables (page 398).

18.10.2 Add runnables

The **eventsubscriber** runnable is an additional component to be deployed on the machine where Matomo is running. You basically need to add two additional runnables to your installation, the **eventsubscriber** runnable itself, and the **cdf** runnable (Cloud Decoupling Framework), which is required for communication between the components. CDF is a queue which can be used to decouple synchronous accesses to services.

This procedure assumes that you will add the **cdf** runnable to your ARIS installation and the **eventsubscriber** runnable to the Matomo server.

Prerequisites

- You have a running ARIS Connect server installation.
- You have access to the remote repository (page 404).
- You have access to the ARIS Agent setup (ARIS DVD 1)
- You have basic knowledge of how to use the ARIS Cloud Controller (ACC).

You always run the ACC connected to your ARIS Agent(s), either using the usual command line switches to connect to a single agent (-h, -u, -pwd) in case of a single node installation or using a node file (passed to the ACC with a -n switch) or by manually issuing **add node** commands in case of a distributed installation.

- Start ACC using the start menu shortcut that was created with setup. Otherwise make sure to always pass in the proper **generated.apptypes.cfg** file to this ACC using the **-c** command line switch. It is important that the **generated.apptypes.cfg** file is of the same version as the version of the installation to which you want to add the runnables.
- Make sure to open specific ports between the ARIS Server and the server where the **eventsubscriber** runnable will be running. These are the **zookeeper** client port and the **ActiveMQPort** of the **cdf** runnable.
- You have access to the Matomo configuration values (IDs and token) (page 397).

Procedure

1. Start ARIS Cloud Controller (ACC) (page 401) on your ARIS Server.
2. Enter the agent user's password.
3. Make the ARIS Agent use the remote repository for downloading the runnables from (page 404).
4. If you have installed the ARIS server using the setup, the ARIS Agent will be set to only take runnables from its local repository, to change that run the command:

```
set local.repository.only=false
```

The ARIS Agent will use the provided remote repository.

5. To add the **CDF** runnable, enter the command:

Example:

```
configure cdf_m cdf_m
```

Note that different from most runnables, the sizing **m** or **l** that you choose does not matter for the **CDF** runnable.

When adding the **CDF** runnable, you will not be able to update this installation with an update setup. As the setup will recognize that the installation has been tampered with. You can either update the installation manually (see **ARIS Update Cookbook**) or you can remove the runnable with the ACC **deconfigure** command (see ACC help), then run the update setup and add and configure the new version of the **CDF** runnable again.

6. Enable usage tracking in all **abs** runnable instances and in all **copernicus** runnable instances. Enter, for example:

```
reconfigure abs_m JAVA-Dcom.softwareag.copernicus.tracking.enabled=true  
reconfigure copernicus_m  
JAVA-Dcom.softwareag.copernicus.tracking.enabled=true
```

7. Install ARIS Agent on the machine where Matomo is installed. The ARIS Agent setup is available on DVD.

This makes ACC available on this machine.

8. To add the **eventsubscriber** runnable to the Matomo server, start ACC and issue the command, for example:

```
configure eventssubscriber_m eventssubscriber_m
```

9. Reconfigure **zookeeper.connect.string** to point to all machines with a ZooKeeper instance, for example:

```
reconfigure eventssubscriber_m  
zookeeper.connect.string="arisapp33srv.eur.com:14281, arisapp45srv.eur.com:14281, <host>:<port>, ..."
```

The **eventssubscriber** runnable will access Matomo via **http://localhost:80/**. If this default is not sufficient, reconfigure **piwik.server.host**, **piwik.server.port**, and **piwik.server.path** accordingly, for example:

```
reconfigure eventssubscriber_m piwik.server.host="arisapp44srv.eur.com"  
piwik.server.port=8080 piwik.server.path="piwik"
```

10. Reconfigure **piwik.site.id** to the ID of the **ARIS Connect** website in Matomo (see saved parameters from Matomo installation (page 397)), for example:

```
reconfigure eventssubscriber_m piwik.site.id=1
```

11. Reconfigure **piwik.visit.tenant.dimension.id**, **piwik.visit.action.resource.path.dimension.id**, and **piwik.visit.action.resource.type.dimension.id** to the IDs of the tenant, resource-path, and resource-type Custom Dimensions that were created in Matomo, for example:

```
reconfigure eventssubscriber_m piwik.visit.tenant.dimension.id=1  
piwik.visit.action.resource.path.dimension.id=2  
piwik.visit.action.resource.type.dimension.id=3
```

12. Reconfigure **piwik.authentication.token** and set the authentication token of an appropriate Matomo user with view permissions for the **ARIS Connect** website (see saved parameters from Matomo installation (page 397)). It is advisable to mask the value of the property with the **?=** reconfigure operator in ACC, for example:

```
reconfigure eventssubscriber_m  
piwik.authentication.token?="f722a764407aef36bf212c6665e53500"
```

13. For the changes to become effective, you need to stop and restart **eventssubscriber** runnable.

The runnables are available. Make sure that they are running.

To use the Matomo reports in ARIS, you must specify the report parameters accordingly (page 405).

18.10.3 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 (<http://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**

18.10.4 Make an ARIS remote repository available

A remote repository is an actual server holding the runnables, but it can also be a local directory in case you don't have a server available. The remote ARIS repository is made available during the setup process. Therefore, an http server is installed temporarily.

To add runnables (page 398) to an ARIS Agent that has not installed an instance of this particular type yet, you must make the ARIS Agent use the remote repository that contains the runnables in question:

1. Start ARIS Cloud Controller (**ACC**). Under a Windows operating system, click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**.

To start ACC under a Linux operating system, execute the **acc.sh** shell script instead.

2. Enter the password of the ARIS Agent user.
3. Make the ARIS Agent use the remote repository to download the runnables. Enter:

set remote.repository.url = "<remoteRepositoryURL>"

When using a local repository, enter, for example:

set remote.repository.url = "file://d:/arisrepo/Setup_Data"

When using a server-based repository, enter, for example:

set remote.repository.url = http://internal.mycompany.com/arisrepo

4. If you have installed the ARIS server using the setup, the ARIS Agent will be set to only take runnables from its local repository, to change that run the command:

set local.repository.only=false

The ARIS Agent will use the provided remote repository.

FILE-BASED REPOSITORY

The simplest approach is to simply copy the contents of the folder **<DVD1_Root>\Windows setups\Setup_Data** from the installation media to a physical drive on the machine to which you want to add the runnables, for example **d:\arisrepo\Setup_Data**. In this example, the URL to your remote repository would be **"file://d:/arisrepo/Setup_Data"**.

SERVER-BASED REMOTE REPOSITORY

If you have a distributed installation, you might want to use a remote repository, which can be any HTTP or FTP server that is reachable from the machine to which you want to add runnables. In that case, simply copy the contents of the folder **<DVD1_Root>\Windows setups\Setup_Data** to your HTTP or FTP server into a suitable location.

If you use an HTTP server whose URL is **http://internal.mycompany.com** and you copy the files to the **arisrepo\Setup_Data** subfolder in the document root of that HTTP server, the URL to your ARIS repository will be

http://internal.mycompany.com/arisrepo/Setup_Data.

18.10.5 How to specify ARIS Aware Matomo reports

You can configure two Matomo-related reports in ARIS Architect. To keep ARIS document storage data up to date, the reports are to be run frequently (page 394).

- The **Matomo - Global portal usage** report (page 408)
Retrieves a set of Matomo reports that collect global ARIS Connect portal usage statistics from Matomo and uploads them to ARIS document storage (Dashboarding/Matomo).
Since a context is mandatory for ARIS reports, an ARIS database must be specified as context for this report. However, the database will not be evaluated by the report and it therefore does not matter which database is selected.
- The **Matomo - Database-specific** report (page 407)
Retrieves a set of Matomo reports that collect database-specific ARIS Connect portal usage statistics from Matomo and uploads them to ARIS document storage (Dashboarding/<database name>/Matomo). Therefore, the database for which it should collect the statistics for must be available and specified as context.

The reports must be parameterized accordingly before they can be executed successfully. If the parameters are invalid, the connection to Matomo fails or the Matomo configuration (page 397) is invalid for usage with ARIS, both reports will fail silently. Errors and warnings are logged (see **jsreport.log** of the runnable executing the report, for example, **abs** or **hds**).

Specify the following parameters according to the parameters specified when Matomo was set up and configured to use ARIS (page 397).

- **Server_Host:** Hostname or IP address of the Matomo server host. The default is **localhost**.
- **Server_Port:** Port of the Matomo service. The default is **80**.
- **Server_Path:** Path of the Matomo service. The default is the root context **/**.
- **Authentication_Token:** Authentication token of an appropriate Matomo user with view permission for the **ARIS Connect** website. The default is **anonymous**. This only works if the anonymous user has view permission.
- **Site_Id:** The ID of the **ARIS Connect** website in Matomo. The default is **1**.
- **Site_Visit_Tenant_Dimension_Id:** The ID of the **tenant** Custom Dimension that was created in Matomo. The default is **1**.

- **Site_Visit_Action_Resource_Path_Dimension_Id:** The ID of the **resource-path** Custom Dimension that was created in Matomo. The default is **2**.
- **Site_Visit_Action_Resource_Type_Dimension_Id:** The ID of the **resource-type** Custom Dimension that was created in Matomo. The default is **3**.

18.10.6 Report: Matomo - Database-specific portal usage

This report creates ARIS database-specific portal usage statistics. Therefore, it accesses an external Matomo instance that contains a collection of ARIS portal events, retrieves specific Matomo reports, and adds ARIS data to them, if required.

The following Matomo reports are retrieved:

- **PageTitles** report
- **CustomDimension** report
- **SiteSearchKeywords** report

To use the Matomo - Global portal usage (page 408) and Matomo - Database-specific portal usage (page 407) reports, make sure to have Matomo installed and configured (page 397) and the report parameters specified accordingly (page 405).

OUTPUT

Generates several **XML** documents stored in the ARIS document storage/Dashboarding/<database name; default=United Motor Group>/**Matomo** subgroup.

The report result is used as input for the Matomo - Publications dashboard.

CONTEXT

Database

18.10.7 Report: Matomo - Global portal usage

This report creates global portal usage statistics. Therefore, it accesses an external Matomo instance that contains a collection of ARIS portal events, retrieves specific **Matomo** reports, and adds ARIS data to them, if required.

The following **Matomo** reports are retrieved:

- **VisitsSummary** report
- **BrowserVersions** report
- **BrowserEngines** report
- **Language** report
- **OsVersions** report

To use the Matomo - Global portal usage (page 408) and Matomo - Database-specific portal usage (page 407) reports, make sure to have Matomo installed and configured (page 397) and the report parameters specified accordingly (page 405).

The parameters must be specified according to the required Matomo settings. If the settings are specified several output files are generated.

OUTPUT

Generates several **XML** documents stored in this subfolder: ARIS document storage/Dashboarding/**Matomo** (page 76).

The report result is used as input for the Matomo - Technical KPIs dashboard.

CONTEXT

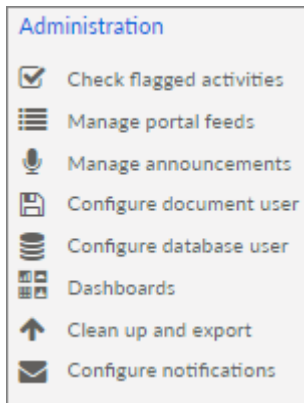
Database

Since a context is mandatory for ARIS reports, an ARIS database must be specified as context for this report. However, the database will not be evaluated by the report and it therefore does not matter which database is selected.

19 Administrate 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. As an Collaboration administrator you have several options (page 420) for managing Collaboration.




19.1 Open Collaboration

Open Collaboration to exchange information, share knowledge, etc.

Prerequisites

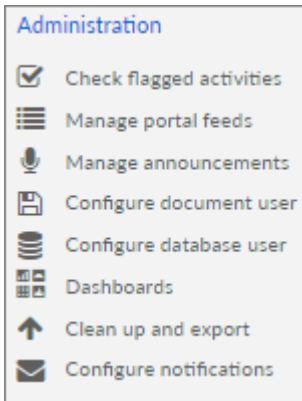
- Collaboration is enabled in ARIS Administration configuration ( **Application launcher** >  **Administration** >  **Configuration** > **Collaboration** > **General settings** > **Activate Collaboration**).
- You have at least the **ARIS Connect Viewer** license privilege.
- You have the required database access privilege (page 422).

Procedure

1. Open ARIS Connect and log in with your user name and password.
2. Click  **Application launcher** >  **Collaboration**.

Collaboration opens.

As an Collaboration administrator you have several options (page 420) for managing Collaboration.







19.2 Check activities flagged as inappropriate

Check content flagged as inappropriate and decide whether it must be deleted.

Prerequisite

- Flagging activities is enabled in ARIS Administration configuration ( **ARIS Administration** >  **Configuration** > **Collaboration** > **General settings** > **Flag activities**).
- You have the **Collaboration administrator** function privilege.

Procedure

1. Under **Administration**, click  **Check flagged activities**. The activities flagged as inappropriate are displayed.
2. Verify whether the Collaboration terms of use have been violated.
3. Click  **Allow** if the content does not violate the terms of use.
4. Click  **Comment** to enter a comment or further information for a post.
5. Click  **Delete** if the content violates the terms of use, and then click **OK**.

The flagged activity was checked and is either deleted or will continue to be shown depending on the result. Alternatively, you can check the flagged activities in your notifications.



19.3 Manage portal feeds


Edit portal feed subscriptions of Collaboration users. You can cancel subscriptions completely or just for individual users. Canceled subscriptions cannot be added here again.

Prerequisite

- You have the **Collaboration administrator** function privilege.
- You have the required database access privilege (page 422).

Procedure

1. Under **Administration**, click  **Manage portal feeds**. The followed items are displayed.
2. Click **Delete** to unsubscribe from a portal feed. This removes the entire stream along with all activities and posts.
3. Click **OK**.
4. To cancel the subscription for individual followers, click **Edit** in the row for the relevant item. The followers are displayed.
5. Click **Unfollow** in the row for the follower whose subscription you want to cancel.
6. Click **OK**.
7. Click  **Save**.

The selected subscriptions will be canceled. The corresponding feed is no longer displayed in  **My portal feeds** for the selected users.

19.4 Synchronize access privileges

For some interactions in Collaboration, users need special access privileges, for example, to post on portal feeds. These access privileges are assigned (page 41) in ARIS Administration or in ARIS Architect. To use updated privileges at once, synchronize them manually in Collaboration.

Prerequisite

- You have the **Collaboration administrator** function privilege.
- You have the required database access privilege (page 422).

Procedure

1. Under **Administration**, click  **Manage portal feeds**.
2. Click **Synchronize privileges**.
3. Click **Execute**.

The access privileges from ARIS Architect are updated. The users can now work with the relevant content.


19.5 Manage announcements

Publish information important for all colleagues as an announcement. Announcements are always displayed on the top of any feed or stream of all users. Additionally, they are highlighted by the background color. Only one announcement is possible at a time, that is, if a new announcement is published, it replaces the previous one.

Prerequisite

- You have the **Collaboration administrator** function privilege.
- You have the required database access privilege (page 422).

Procedure

1. Under **Administration**, click  **Manage announcements**.
2. Enter the announcement title.
3. Enter or copy your text into the text box. Up to 2000 characters are available.
4. Click **OK**.

Your announcement is published in **All company feed** and **My feed** of all colleagues. Users can hide the announcement in their feed by clicking  **Remove**.

If the announcement is outdated, delete it (**Administration** >  **Manage announcements**).

19.6 Configure ARIS document storage user

Specify a user responsible for the generation of dashboards. The data of dashboards is stored in ARIS document storage. The dashboard data from Collaboration is automatically updated to ARIS document storage every day. Only one ARIS document storage user (page 78) can be specified at a time. For detailed information about access to ARIS document storage (page 78), please refer to **Manage documents** help.

Prerequisite

- You have the **Collaboration administrator** function privilege.
- You have the **Dashboard administrator** function privilege.
- You have the **ARIS Connect Designer** license privileges.



Procedure

1. Under **Administration** click  **Configure document user**.

2. Enter the user name and the password of the relevant user.
3. Click **OK**.

The ARIS document storage user is specified.


19.7 Configure database user

Specify a user responsible for the interaction with ARIS Connect server. The users login information is required for processes executed in the background, for example, the activation of automatic following ( **Application launcher** >  **Administration** > **Collaboration** > **Configure database user**). Only one database user can be specified at a time.

Prerequisite

- You have the **Collaboration administrator** function privilege.
- You have the ARIS Connect Designer license privilege.
- The user to be configured as database user must have the **Database administrator** function privilege.

Procedure

1. Under **Administration**, click  **Configure database user**.
2. Enter the user name and the password of the relevant user.
3. Click **OK**.

The database user is specified.

19.8 Display dashboards

You can view statistics data using dashboards. Dashboards can be used, for example, to perform controls in real time.

Prerequisite

- You have the **Collaboration administrator** function privilege.
- You have at least the **MashZone Viewer** license privilege.
- **Generate user statistics (com.aris.umc.audit.enabled)** is enabled in the configuration (page 244) (**User management** > **Security** > **Advanced settings**). If **License monitoring (User management > License monitoring > General)** is enabled, **Generate user statistics** is automatically enabled.

- Your ARIS Server is enabled for ARIS Aware.
- ARIS document storage user is specified (page 412).

Procedure

1. Under **Administration**, click  **Dashboards**.
2. Click the relevant area (**Overview, Content, Users, Groups**).

The dashboards for the selected area are displayed.



More information on dashboards is available in Use dashboards, Dashboards available by default, and Set up dashboards.

Example




19.9 Clean up and export activities

You can delete activities from before a specified date in order to remove outdated content from Collaboration. This makes the feed overview more transparent. To archive this data, you can create an export. These elements are stored in the export: Comments, tags including hashtags and system tags, external links, links to models, bookmarks, likes, etc.



Depending on the configuration, the activities are exported as a ZIP file or the ZIP file is stored in ARIS document storage and you can download it later ( **Application launcher** > 

Administration >  **Configuration** > **Collaboration** > **General settings** > **Export activities as a ZIP file instantly**).


Procedure

1. Under **Administration**, click  **Clean up and export**.
2. Click the **Activities older than** box. The calendar opens.
3. Select the date from which all earlier activities are to be deleted or exported.
4. Click **OK**.
5. Specify whether the activities should be exported and/or deleted.
6. Depending on your selection, click **Export**, **Export and delete** or **Delete**.

According to your specifications, the activities older than the date entered are deleted and/or exported. The export is saved as a ZIP file.

Archive the ZIP file on your computer. To do so, move the mouse pointer over the relevant export. The buttons of the available functions are displayed. Click  **Download ZIP file**. If export files are outdated, you can remove them from the list by clicking on  **Delete Zip file**.

19.10 Configure notifications

You can specify the time for daily e-mail notifications and the day for weekly e-mail notifications. Defaults are AM 00:00 and Monday respectively. The global settings are used for all users who have not specified an e-mail frequency in their own account yet ( **View notifications > Change your notification settings**).

Prerequisite

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

Procedure

1. Under **Administration**, click  **Configure notifications**.
2. Select a time for the daily digest e-mail (**Daily digest at**).
3. Select a day for the weekly digest e-mail (**Weekly digest on**).
4. Select a global frequency (**Global settings**).
5. Click **Save**.

The e-mail notifications will be sent to the users at the time and on the day you specified.


19.11 Customize e-mail notifications

You can customize the e-mail notification layout by editing the HTML template. You can, for example, adapt font size and font color as well as the background color.


Prerequisite

- You have the **Collaboration administrator** function privilege.
- You know how to edit HTML code.


Procedure

1. Under **Administration**, click  **Configure notifications**.
2. Click **Customization**. The HTML template is displayed.
3. Edit existing HTML tags or add new ones. See the example below.
4. Under the HTML template, click  **Help** to receive information about important keywords used in the HTML template.
5. Click  **Save**.
6. Under the HTML template, click  **Send preview e-mail** to receive an e-mail with a preview of your customized design.

The customized layout is created.

Click  **Restore defaults** below the HTML template to undo all the settings you have made. The default settings are loaded and the template is refreshed.

Tip

Alternatively, you can edit the template with an external HTML editor. To do so, copy the template to your clipboard ().

Example


Change the background color of the e-mail and the heading.

- Replace the tag `<body class="mail-font-family">` with `<body class="mail-font-family" style="background-color: #0899CC;">` in order to use a blue background color.
- Replace the tag `<h3 class="mail-heading body-heading">$emailTitle</h3>` with `<h3 class="mail-heading body-heading">My customized e-mail template</h3>` in order to use the heading **My customized e-mail template**.

Your preview e-mail should now look like this:

ARIS Connect

My customized e-mail template

 **Tom Tailor** posted a **message** to your feed.

This is a preview message to test the layout.

Tuesday, February 28, 2017, 08:44 AM

[Open Collaboration](#) | [Change frequency of notifications](#) | [Help](#)




You are receiving emails from ARIS Connect Collaboration.

Copyright © 2012 - 2017 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.

19.12 Keyboard shortcuts for Collaboration

The following shortcuts are available in Collaboration.

Keyboard shortcuts can be performed on selected items. Selected items can be identified by the focus in the program.

Shortcut	Action
Page down	Scrolls the screen down. The scroll distance may vary depending on the application.
End	Moves to the lower entries if they cannot be displayed completely due to the window size or the screen resolution.
Page up	Scrolls the screen up. The scroll distance may vary depending on the application.
Home	Moves to the upper entries if they cannot be displayed completely due to the window size or the screen resolution.
Tab	<ul style="list-style-type: none"> ▪ Opens the navigation for page sections if you press Tab immediately after opening the page. ▪ Highlights the next control or input box. ▪ Jumps from the Comment box to the  Tag,  Link, and  File symbols that you can use to attach tags, links, or files to your comment. It also jumps to the other input fields and to the Post button.
Shift + Tab	Highlights the previous control or input box.
Right arrow/ Left arrow	Moves the cursor through the text in input boxes.
Up arrow/ Down arrow	Selects the previous/next item in lists.
Enter	<p>Opens the attachment fields and places the cursor in the input field if the Tag or Link symbol is selected. Opens the Select document dialog when the File symbol is selected.</p> <ul style="list-style-type: none"> ▪ Posts the comment when the Post button is selected. ▪ Executes the highlighted button. ▪ Opens the dialog/the selection list of the highlighted item.
Ctrl + Enter	Posts a comment when the Post button is active.

19.13 Privileges of coordinators and administrators

COORDINATORS

- Are responsible for managing the group profile, privileges, access, and feed activity facilitation.
- Can delete their groups.

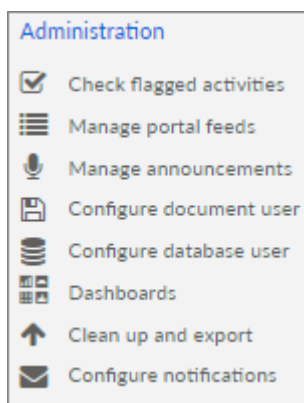
As the creator of a group, you are automatically the coordinator. You can assign coordinator privileges to other group members, as well. If there is no coordinator anymore for a group, for example, because all users with coordinator privileges for a group were deleted, Collaboration administrators can manage the group and assign coordinator privileges.

COLLABORATION ADMINISTRATORS

- Have the same privileges as coordinators.
- Manage the posts that users have flagged as inappropriate (page 410).
- Can synchronize (page 411) access privileges.
- Can manage (page 412) announcements.
- Can configure ARIS document storage user (page 412) and database user (page 413).
- Can assign user groups from ARIS Administration to a Collaboration user group.
- Can display (page 413) dashboards.
- Can clean up and export (page 415) activities.
- Can view all posts and delete them.
- Can configure (page 415) and customize (page 416) e-mail notifications.
- Can customize (page 368) Collaboration in ARIS Administration.

Collaboration administrator is a function privilege assigned in ARIS Administration.

COLLABORATION ADMINISTRATION



19.14 What is the 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 (page 27) 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. The technical name of the synchronization user, for example in ARIS Advanced Controller, is **_aris_tech_user_ecp_techuser**. For detailed information, refer to **ARIS Cloud Controller (ACC) Command-Line Tool**, chapters **Create synchronization user** and **Force synchronize Collaboration users**.

19.15 Delete and anonymize user accounts

Users can only be deleted (page 25) in ARIS Administration. To anonymize Collaboration users according to GDPR, use ARIS Cloud Controller. For detailed information, refer to **ARIS Cloud Controller (ACC) Command-Line Tool**.

After anonymization, activities of Collaboration users, such as posts, comments, groups, are shown with **Anonymized user** instead of with the user name. The same applies to dashboards. To distinguish the anonymized users from each other, a number is automatically added to **Anonymized user**. This number is increased by one for each additional anonymized user, for example, **Anonymized user2**. Pictures of anonymized users are no longer shown. User profiles, bookmarks, filters, etc. of anonymized users in Collaboration are deleted.

19.16 Collaboration dashboards

There are dashboards from the overview, Collaboration content, users and groups areas.

Example



19.17 Database access privileges for Collaboration

For some interactions in Collaboration, users need special access privileges, for example, to post on portal feeds. These access privileges are assigned (page 41) in ARIS Administration or in ARIS Architect. You can synchronize (page 411) the privileges in Collaboration manually, after you edited them in ARIS Architect. The following database access privileges are relevant to Collaboration:

- **No access (----)**
No portal content is displayed.
- **Read (r---)**
Portal content is displayed. Users can read posts added to models, and they can like, share, bookmark, tag, and flag them. However, they cannot comment on models.
- **Read + Comment (rc--), Read + Write (rw--)** (and all other types of rw access)
Portal content is displayed. Users can use all functions of Collaboration.

For detailed information about access privileges, refer to the help in ARIS Architect (ARIS Configuration and Administration).

20 Manage SAP Solutions

Some features of ARIS for SAP® Solutions are available in ARIS Connect, if your ARIS administrator has configured the system in ARIS Connect as well as in ARIS Architect. For details, see **ARIS for SAP® Solutions** manual and **ARIS Requirements for SAP® Solutions** manual available on DVD 3, in the ARIS Download Center (<https://aris.softwareag.com/>) or on Empower (<https://empower.softwareag.com/>).

ARIS video tutorial

Process-Driven SAP Management Explainer, 4 minutes

(<https://resources.softwareag.com/youtube-product-videos-for-uberflip/manage-your-digital-future-support-best-in-class-sap-solutions-with-aris>)



20.1 Import portal configuration set providing SAP content

To start executables and download SAP documents, or to have the ARIS Online Guide available, you must import (page 424) SAP-related configuration sets for the portal and publish the database in **Published content** (page 139, page 427).

Prerequisites

- You have the **Portal administrator** function privilege.
- You have access to the **Add-ons** folder on the installation media **ARIS DVD 3**.

Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**.
3. Click **Portal** > **Manage configuration sets**.
4. Click **Restore**. The file selection dialog opens.
5. Navigate to the **classicSAP.zip** or **defaultSAP.zip** archive file that is located on ARIS DVD 3 (Add-ons/Extension pack SAP/Configuration sets).
6. Double-click the ZIP file.

The imported configuration set is listed.

If you activate this configuration set (page 425) and publish the databases (page 139, page 427), the Run SAP executable, Download SAP documents, and ARIS Online Guide actions are available.





20.2 Select the View Providing SAP Content

Select the **classicSAP** or **defaultSAP** configuration set to display portal data.

Prerequisite

- You have the **ARIS Connect Designer** license privilege.
- You have imported the classicSAP or the defaultSAP view (page 424).
- You have the **Portal publisher** function privilege.

Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**.
3. Click  **Configuration** > **Portal** > **Manage configuration sets**. All available views are displayed. The current view is marked.
4. Move the mouse pointer over the additionally created view, for example, **classicSAP** or **defaultSAP**. If the configuration sets are not available, your Portal administrator must import (page 424) them.
5. Click  **Activate**.

All of the databases selected for the portal are published in the selected view.

20.3 Configure ARIS Online Guide

If the ARIS Online Guide is used for making documents that were created in the SAP® system specially for your business processes available across the company, configure your custom settings to call the ARIS Online Guide.

Prerequisite

ARIS and the SAP® system have been configured for using the ARIS Online Guide.

Procedure

1. Log on to the SAP system.
2. Start the `/n/IDS/AOG_USER` executable. The **ARIS Online Guide - User-specific settings** dialog opens.
3. Enable the **Use ARIS Online Guide** check box.
4. Select the **Connect** option to display the ARIS Online Guide in the portal in ARIS Connect.
5. If you also want to use the F1 help from the SAP system in addition to the ARIS Online Guide, enable the **Also show default help** check box.
6. Enter the required connection data for ARIS Server and tenant on which the database was published as a portal. You administrator might already have specified default entries that you do not need to edit.

Base URL for Connect

URL for the relevant ARIS Server:

http://<server name>

Tenant

Tenant that manages the database published as a portal.

7. Save your changes.

The settings have been applied.

If you changed the default values set by your administrator and want to restore them, click **Restore defaults**.




20.4 Publish databases in ARIS Connect (ARIS Online Guide)

If you plan to use ARIS Online Guide to make documents available across the company which were specially created for your business processes in the SAP® system during customizing, please make the databases available in **Published content** of ARIS Connect.

Prerequisite

- You have the **Database administrator** function privilege.
- You have the **Publishing administrator** function privilege.

Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**.
3. Click **Portal > Publish databases** if it is not already selected. The  **Configuration** tab displays the **Publish databases** area. All available databases are displayed.
4. Enable the check boxes of the databases you want to publish in **Published content**.
5. For versioned databases, select the relevant version.
6. Click **Apply**.






The content of the databases is published in **Published content** in the selected configuration or modification set. If databases are available in **Published content** they cannot be deleted in ARIS.

20.5 Make log files available

After transferring projects/branches or performing SAP synchronization all actions are logged. The files can be opened after each action and will be saved automatically. If log files are not saved in project or solution configurations in ARIS Architect, make sure that, in ARIS document storage configuration, the **txt** file extension is configured as valid extension.

You have the **Technical configuration administrator** function privilege.

Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**.
3. Click  **Configuration**.
4. Click **Document storage**.
5. Select **Quota and restrictions**.
6. Click  **Edit**.
7. Make sure that **txt** is listed in the **Valid file extensions** field, and that the **txt** file type extension is **not** restricted.
8. Click  **Save**.

Log files with **txt** extensions can be transferred.

21 Configure Tenant Management

The Tenant Management user interface has been installed using the ARIS Server setup program. It is run automatically with the user account of the **superuser** user. In order for other users to be able to log in (page 433), you have to configure the infrastructure tenant (page 429). This assigns users in the infrastructure tenant privileges for impersonation (page 147), along with additional function privileges.

Once all operational tenants are configured (page 431), impersonation enables users to assume the account of the **superuser** system user 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 433).



21.1 Configure infrastructure tenant

In order for users to be able to log in to Tenant Management, they must have been assigned **impersonation** privileges (page 147) by a system user 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, for example, **http://myServer:1080/umc**. The User Management login dialog opens.
2. Enter the name of the infrastructure tenant in the  **Tenant** field, for example, **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. Enter a valid e-mail address. This assures that the system administrator is informed whether backups were completed successfully or whether warnings or errors occurred.
7. Click **Privileges**. The list of function privileges is displayed.

8. 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 431).

21.2 Configure user for impersonation

Impersonation enables a user to assume another user account. The user can then perform operations that are actually only permitted for the other account. This configuration must be set for each tenant.

Prerequisite

You have the **Technical configuration administrator** function privilege.

Procedure

1. Log in to User Management.

Click the link that was provided to you or that you have saved as a bookmark in your browser, for example, **http://myServer:1080/#myTenant/adminUsers**. The **Log in** dialog opens.

2. Enter the name of the infrastructure tenant in the  **Tenant** field, for example, **master**.

3. Enter your user name and your password.

4. Click the user for which you want to allow impersonation.

5. Click **Privileges**. The list of function privileges is displayed.

6. Click the user for which you want to allow impersonation.


7. Activate the **Impersonation** function privilege.

8. Log out.

9. Log in (page 3) to ARIS Connect.

10. Click  **Application launcher** >  **Administration**. The **Administration** view opens.

11. Click  **Configuration**.

12. Click **User management**.
13. Click the arrow next to **Users**.
14. Click **General**.
15. Click  **Edit**.
16. Click in the **Impersonation target users** field.
17. Enter the users for which you want to allow impersonation as a comma-separated list.

Warning

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

18. Click  **Save**.

You have allowed users to use impersonation.

21.3 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, for example, `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 your name > **Administration**. ARIS Administration opens.
4. Click  **Configuration**.
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
 - ARCM administrator
 - Collaboration administrator
 - Database administrator
 - Dashboard administrator
 - Document administrator
 - License administrator
 - Portal 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 435). All substitutes can log in using their user name and manage tenants on behalf of the system user **superuser**.

21.4 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.

Add missing permissions to the superuser, if impersonation (page 147) failed. This can occur, if tenants were added by ARIS Cloud Controller (ACC) but functional privileges are missing.

Procedure

1. Click **Tenants**. The status of the tenants is displayed. If the **● Impersonation failed** status is shown, the tenant is not accessible for users.
2. At the end of the row for the tenant, click **⋮ More > Allow access**. The **Allow access** dialog opens.
3. Enter the user credentials of a user with sufficient privileges, for example, **system**.
4. Click **OK**.

The missing privileges are applied to the superuser. Impersonation should work and the **● Active** state is shown. If the change is not displayed, click **🔄 Refresh**.

21.5 Open Tenant Management

System users and users (page 429) 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 (page 429).

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.

Warning

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

4. Click **Log in**.

You can manage all tenants in the system.

21.6 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 147).

21.7 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, for example, master (page 146). 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, for example, **default**, the user **superuser** must be defined as the target for impersonation (page 429). Impersonation enables users to back up tenants in which they do not exist as a user.


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

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

21.8 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 and if all components were selected for the backup. Extensions, for example, TLS/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.

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 User statistics in backup (com.aris.umc.user.statistics.backup) must be enabled in the configuration (page 244) (see ARIS help: ARIS Administration >  Configuration > User management > Security > Advanced settings).</p>	<p>User administrator</p> <p>Technical configuration administrator</p>	<p>ARIS Administration/User Management</p> <p>(umcadmin_<s, m, or l>)</p>
<p>Licenses</p> <p>User administration audit events are not part of the tenant backup.</p>	<p>License administrator</p>	

Content	Required function privileges	Component (runnable)
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, including Process Governance archives 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 and feeds	Dashboard administrator	ARIS Aware (dashboarding_<s, m, or l>)
ARIS Connect portal views, modification sets, and configuration sets.	Portal administrator	ARIS Connect portal (copernicus_<s, m, or l>)

Make sure to save backup files on external media, such as a NAS or file servers. You require the same function privileges to restore the data.

22 Legal information

22.1 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.

22.2 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.

SOFTWARE AG EMPOWER PORTAL

You can find documentation on the Software AG Documentation website (<https://empower.softwareag.com/>). The site requires credentials for Software AG's Product Support site **Empower**. If you do not yet have an account for **Empower**, send an e-mail to empower@softwareag.com with your name, company, and company e-mail address and request an account.

If you have no account, you can use numerous links on the TECHcommunity website. For any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory and give us a call.

TECHCOMMUNITY

On the **TECHcommunity** website, you can find documentation and other technical information:

- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Access articles, code samples, demos, and tutorials.
- Find links to external websites that discuss open standards and web technology.
- Access product documentation, if you have **TECHcommunity** credentials. If you do not, you will need to register and specify **Documentation** as an area of interest.

EMPOWER (LOGIN REQUIRED)

If you have an account for **Empower**, use the following sites to find detailed information or get support:

- You can find product information on the Software AG Empower Product Support website.
- To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the Knowledge Center.
- Once you have an account, you can open Support Incidents online via the eService section of Empower.
- To submit feature/enhancement requests, get information about product availability, and download products, go to Products.

SOFTWARE AG MANAGED LEARNINGS

Get more information and trainings to learn from your laptop computer, tablet or smartphone. Get the knowledge you need to succeed and make each and every project a success with expert training from Software AG.

If you do not have an account, register as a customer or as a partner.

23 Index

A

- ARIS document storage
 - Export • 289
 - Full-text search • 323
 - Import • 288
 - Infrastructure • 290
 - Permanent document • 83
 - Properties • 72
 - Quota and restrictions • 319
 - Temporary document • 83
 - Third-party document management system • 302
 - WebDAV • 330

C

- Chart
 - Display • 137
- Collaboration
 - Check activities reported • 410
 - Clean up and export activities • 415
 - Configuration • 368
 - Configure ARIS document storage user • 412
 - Configure database user • 413
 - Configure notifications • 416
 - Configure synchronization user • 421
 - Customize e-mail notifications • 417
 - Delete and anonymize users • 421
 - Display dashboards • 413
 - Manage announcements • 412
 - Manage followers • 411
 - Open Collaboration • 409
 - Synchronize access privileges • 411
- Configuration
 - Collaboration • 368
 - Export • 146
 - Impersonation user • 146
 - Import • 145
 - System configuration • 139
- Coordinator
 - Privilege • 420

D

- Database
 - Default • 142
 - Function privileges • 33
 - Sort order • 141
- Document
 - Permanent document • 83
 - Properties • 72
 - Temporary document • 83

F

- Folder
 - Create folder • 76
 - Properties • 76
 - Restrict access • 78

G

- GDPR
 - Anonymize • 64

K

- Keyboard shortcuts
 - Collaboration • 419

L

- LDAP
 - Import users • 52
 - Synchronize items • 53
- Licenses
 - Create license rule • 7
 - Delete • 7
 - Dependencies • 4
 - Display • 5
 - Download/upload license rules • 9
 - Enable/disable license monitoring • 6
 - Expired • 6
 - Generate license audit report • 10
 - Generate license usage rule validation report • 11
 - Import • 5
 - Rule types • 8
 - Types • 4

P

Portal

- Assign a portal profile • 44
- Portal profiles • 66
- Publish database • 140
- Show SAP content • 424

Privileges

- Assign/remove a privilege • 40
- Change assignment • 41
- Change privileges • 41
- Default users • 27
- Function privileges • 33, 45

Process administration

- Archive • 105
- Assignments • 106
- Console • 106
- Contents • 103
- Context • 106
- Correct/restart failed instances • 127
- Delegate human tasks • 130
- Delete process • 117
- Details • 106
- Diagram • 107
- Display human tasks • 129
- Exclusive licenses for user groups • 44
- Executable processes • 128
- Find failed instances • 122
- Find process instances • 111
- History • 107
- Human tasks • 108
- Information about activities • 129
- Information about variables • 130
- Instances • 109
- Notifications to Process Governance administrators • 333
- Number of process instances • 113
- Open • 103
- Priority of process instances • 120
- Process instance archive • 118
- Reminder about human tasks • 114
- Restart failed activities • 124
- Retrieve information • 128
- Review input and output data • 123
- Skip failed activities • 125
- Skip human tasks • 126

- Status of activities • 132
- Status of process instances • 133
- Suspend recurrence • 116
- Suspend/resume process instance • 114
- Task state • 134
- Tasks • 110
- Terminate process instance • 115

Process Governance

- Infrastructure • 344
- Notifications • 333
- Pools • 363
- Publishing • 353
- Reporting • 356

Profile

- Assign a portal profile • 44

S

SAP

- Configure ARIS Online Guide • 426

SCIM

- Copy bearer token • 55
- Customize settings • 270
- Delete bearer token • 56
- Generate bearer token • 54
- SCIM keys • 274

Server tasks

- Cancel report • 382
- Completed tasks list • 384
- Display • 381
- Running tasks list • 383
- Server tasks area • 383
- Toggle auto-refresh • 381

U

User

- Anonymize • 64
- Change password • 50
- Create • 18
- Delete • 26
- Edit • 24
- Log out by administrator • 25

User groups

- Copy • 37
- Create • 36
- Delete • 39
- Edit • 38

User management

- Assign user group to user • 23
- Assign users to a user group • 38
- Back up data • 57
- Default users • 27
- Delete all • 27
- Export statistics • 58
- Generate license audit report • 10
- Generate license usage rule validation report • 11
- Generate report • 59
- Impersonation user • 146
- Information on users/user groups • 62
- Infrastructure • 150
- Kerberos • 157
- LDAP • 167
- LDAP server operations • 168
- Log out by administrator • 25
- Password policy • 218
- Restore user management data • 58
- Security • 243
- SMTP • 254
- User-defined notifications • 200
- Users • 261

V

View

- Show SAP content • 424