software AG

ARIS

USERS AND LICENSE MANAGEMENT

Version 10.0 - Service Release 2

October 2017

Contents

1   Legal notices

This manual describes the settings and features as they were at the time of print. Since manual 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 Readme file that accompanies the product. Please read this file and take the information into account when installing, setting up, and using the product.

If you want to install all technical and/or business system functions without the services of 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 only describe specific installations. It is not possible to document all settings and dependencies.

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

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

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

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

2   Text conventions

Menu items, file names, etc. are indicated in texts as follows:

- Menu items, key combinations, dialogs, file names, entries, etc. are displayed in **bold**.

- User-defined entries are shown **<in bold and in angle brackets>**.

- Single-line example texts (e.g., a long directory path that covers several lines due to a lack of space) are separated by ↵ at the end of the line.

- File extracts are shown in this font format:

  `This paragraph contains a file extract.`

- Warnings have a colored background:

  Warning

  This paragraph contains a warning.

3   Users and licenses

For all ARIS products users are managed centrally within the user management. Using ARIS Server the user management is part of the ARIS Administration. The role specific data access is handled by license privileges and function privileges and database specific privileges managed within the ARIS Administration and database specific privileges and filters associated to users and user groups. These database specific privileges and filters are managed within ARIS Architect for each database of a tenant.

After the ARIS Server installation the **superuser** user can only login to the ARIS Administration. The initial password is **superuser**. Also the **system** user can do so, using the initial password **manager**. Both users hold sufficient permissions to manage users and licenses. The superuser only has these permissions and cannot login to ARIS Download Client or ARIS Connect as no license can be assigned. The **system** user holds all permissions to manage all data in the system. This user only needs to get licenses assigned to do so.

If you are about to make the Tenant Management interface available, the superuser needs additional permissions in the infrastructure tenant as well as in all operating tenants.

USER MANAGEMENT WITHIN THE ARIS ADMINISTRATION

The ARIS Administration is a tool managing users, user groups, privileges, licenses, documents, and configurations for each tenant affecting all ARIS products. This ensures the single sign-on for various ARIS products. Users can also be imported from an LDAP system. ARIS Administration is available for users holding the **User administrator** and **License administrator** function privilege. Initially, only the administrative users **superuser** and **system** are available. These users are able to manage users for all tenants of your system (page 3). Users can also be managed using the ARIS Administration's command line tools.

If you are going to manage users within the ARIS Administration make sure to have the ARIS Risk & Compliance Manager reconfigured and that you have forced ARIS Publisher Server to use the specific ARIS Administration.

Administrators must perform these actions in order to allow access to ARIS:

1.   Change the passwords of the **superuser** user and the **system** user. (page 9)

2.   Import the license if it has not been imported during the setup process.

3.   Create users or import them from the LDAP system.

4.   Create user groups or import them from the LDAP system.

5.   Assign users to user groups.

6.   Assign privileges.

    Further information is available in the ARIS Administration's online help.

All users and user groups managed in the ARIS Administration are available in every existing or future databases of the tenant. In each database product specific privileges must be assigned in ARIS Architect. To do so, please also to the ARIS Architect online help chapter **Manage users**.

USER MANAGEMENT WITHIN ARIS ARCHITECT

While creating a database all users and user groups are imported from the ARIS Administration. To control data access and role specific actions administrators need to assign privileges and filters for each database.

Please make sure to have managed users and licenses before you manage users in ARIS Architect.

These actions can be performed by all users holding the function privileges **Database administrator** and **User management**.

1. Create databases.

2. Assign database specific privileges and filters.

3. Provide the URL **http://<IP address or fully-qualified host name>:<load balancer port>/#<tenant name>/home**, e.g. **http://aris.connect.sag/#default/home** to all users using ARIS Connect.

All authorized users have access to licensed ARIS products.

Privileges and filters must be assigned for each additional database.

Further information is available in the ARIS Administration's online help.

4   What is impersonation?

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

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

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

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

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

5   Tenant

After the installation of ARIS Connect or ARIS Design Server two tenants are available. The operational **default** tenant and the infrastructural **master** tenant.

5.1   Log into the infrastructure tenant's User Management

After the installation of ARIS Server, two tenants are available. The operation default tenant and the infrastructural **master** tenant. This **master** tenant works in the background and manages administrative users and all other tenants.

You only need to log into the User Management

- to change the **superuser**'s and the **system** user's passwords to prevent unauthorized access

- to configure the Tenant Management tool

After the installation only the administrative users **superuser** or **system** can login.

Manage users, user groups, privileges, licenses, documents, configurations, and processes for all ARIS products.

For detailed information please refer to the ARIS Administration's online help.

Procedure

1. Click the link **http://localhost/umc** or **<IP address or fully-qualified host name>/umc**. The login dialog of the ARIS Administration opens.

2. Enter the user name **superuser** and the password **superuser**.

3. Change the tenant name if **default** is not the one you want to login to.

4. Click **Log in**.

The ARIS Administration opens.

5.2   Change passwords on the infrastructure tenant

On the infrastructure tenant (**master**), change the passwords of **superuser**, **system** user and **guest** user. This will prevent unauthorized actions within the system. These users are created automatically for each tenant. The **system** user holds all function privileges and access for all databases. The **superuser** user holds all privileges to allow user and license management.

1. Log into the infrastructure tenant's User Management (page 6).

2. Click ⚎ **User management**, and select **Users**. The list of users is displayed.

3. Enter **superuser** into the search box. The search result is shown.

4. Click **superuser**. The user data (details) is displayed.

5. Click ✎ **Edit**.

6. Enable the **Change password** check box. The **Password** and **Confirm password** boxes are displayed.

7. Enter a new password, and reenter it. If you want to use the webMethods integration, passwords may not contain a colon.

8. Click **Save**.

9. Change the **system** user's password too.

The passwords are changed. The users receive e-mail notifications.

5.3   Log into the tenant's ARIS Administration

The ARIS Administration is a tool to manage users, user groups, privileges, licenses, documents, and configurations for each tenant of all ARIS products. This ensures the single sign-on for various ARIS products. Users can also be created using an LDAP system. ARIS Administration and the online help are available for users holding the **User administrator** and **License administrator** function privilege. After the installation only the administrative users **superuser** or **system** can login. For detailed information please refer to the ARIS Administration's online help.

Procedure

1. Open your browser and enter **http://<IP address or fully-qualified host name>:<port number other than default>/#<tenant name>/adminSettings**. You must enter the port number only if you have changed or redirected the standard port **80**. The login dialog opens.

2. Enter the user name **superuser** and the password **superuser**. This user only has access to the server's ARIS Administration.

3. The ARIS Administration's **Configuration > User management** tab opens.

4. Click the required tab.

You can manage users, user groups, privileges licenses documents and the configuration of this tenant.

5.4 Change passwords on tenants

On all tenants, change the passwords of **superuser** user, **system** user and the **guest** user. This will prevent unauthorized actions within the system. These users are created automatically for each tenant. The **system** user holds all function privileges and access for all databases. The **superuser** user holds all privileges to allow user and license management.

1. Log into the tenant's ARIS Administration (page 8).

2. Click **User management**, and select **Users**. The list of users is displayed.

3. Enter **superuser** into the search box. The search result is shown.

4. Click **superuser**. The user data (details) is displayed.

5. Click **Edit**.

6. Enable the **Change password** check box. The **Password** and **Confirm password** boxes are displayed.

7. Enter a new password, and reenter it. If you want to use the webMethods integration, passwords may not contain a colon.

8. Click **Save**.

9. Change the **system** user's password too.

The passwords are changed. The users receive e-mail notifications.

6 Configure single sign-on

You can configure single sign-on (SSO) using Kerberos (page 10) or SAML (page 17).

When using Kerberos, this provides access to all ARIS runnables as soon as a user has logged in to the domain.

When using SAML, this provides access to all ARIS Connect runnables as soon as a user has logged in to the domain.

However, if you use ARIS Publisher you must reconfigure the **businesspublisher** runnable and only Kerberos is supported.

6.1 Configure Single Sign-On using Kerberos

If you are using LDAP, you can configure SSO (single sign-on). This enables access to all ARIS runnables as soon as a user has logged in once to the domain.

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 MS Windows networks. In addition, it is widely used with Linux operating systems and is designed for use with all major platforms. It is designed to provide a strong authentication for client/server applications, like web applications where the browser is the client. It is also the recommended way to authenticate users in a MS Windows network and it replaces the outdated and relatively insecure NT LAN Manager (NTLM).

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>**, e.g. **HTTP/mypc01.my.domain.com**.

Client

- The client computers and servers are connected to the same MS Active Directory Domain Services.

- The browser used supports a Kerberos-based authentication.

- The browser has been configured accordingly.

The following steps must be taken to use SSO:

Procedure

1. A technical user must be created in the MS Active Directory.

2. A service principal name must be registered on the technical user.

3. The Single Sign-On configuration options must be set in the ARIS Administration.

4. The client application must be configured to use Single Sign-On.

You configured SSO on client side.

CREATING A TECHNICAL USER

A technical user is used to validate Kerberos tickets against the Microsoft Active Directory. This user must be created in the Microsoft Active Directory and a keytab file must be created for this user.

A keytab file contains a list of keys and principals. It is used to log on the technical user to the Microsoft Active Directory without being prompted for a password. The most common use of keytab files is to allow scripts to authenticate against the Microsoft Active Directory without human interaction or storing a password in a plain text file. Anyone with read permission on a keytab can use all of the keys contained so you must restrict and monitor permissions on any keytab file you create. The keytab must be recreated when the password of the technical user changes.

A keytab file can be created by passing the following parameters to the **ktab.exe** JRE command line tool:

ktab -a <TECHUSER_USER_PRINCIPAL_NAME> -n 0 -append -k umc.keytab - e.g. **ktab –a aristechuser@MYDOMAIN.COM –n0 –append –k umc.keytab**.

CONFIGURATION OPTIONS IN ARIS ADMINISTRATION

You need to configure SSO for the servers.

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

Procedure

1. Log in to the ARIS Administration.
2. Click the arrow next to your name.
3. Click **Administration**.
4. Click **Configuration**.
5. Switch to **User management**.
6. Click the arrow next to **Kerberos**.
7. 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_enctypes = 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_enctypes = 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_enctypes = 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
   ```

8. To upload the configuration file, click 📤 **Upload** under the **Configuration file** field.
9. Click 🖊 **Edit**.
10. Enable **Use Kerberos**.
11. 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.

12. In the **Realm** field, configure the realm for the Kerberos service. Enter the fully qualified domain name in uppercase letters.

    Example: **MYDOMAIN.COM**.

13. In the **KDC** field, configure the fully qualified name of the KDC to be used.
14. **Optional:**

    a. Click **Advanced settings**.

    b. Enable **Debug output**.

       The debug output of the program that the user wishes to log in to 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.

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®

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 it back in.

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.

6.2   Kerberos keys

You can configure Kerberos as required.

Key	Description	Valid input	Example
com.aris.umc.kerberos.active	Use Kerberos Specifies whether a Kerberos-based login is allowed.	true, false	
com.aris.umc.kerberos.config	Configuration file Storage location of the configuration file for Kerberos. The file can be uploaded directly.	String	./config/Kerberos/krb5.conf
com.aris.umc.kerberos.debug	Debug output Specifies whether debug output is allowed for Kerberos operations.	true, false	
com.aris.umc.kerberos.kdc	KDC Specifies the fully qualified name of the central **K**ey **D**istribution **C**enter (**KDC**). This is usually the fully qualified host name of the LDAP server.	String	049bfs01.me.corp.softwareag.com
com.aris.umc.kerberos.keyTab	Key table Specifies the location of the keytab file that is used for Kerberos tickets. The file can be uploaded directly.	String	C:/safePlace/krb-umc.keytab
com.aris.umc.kerberos.realm	Realm Specifies the realm of Kerberos tickets. Fully qualified domain name in uppercase letters.	String	MY.CORP.SOFTWAREAG.COM

Key	Description	Valid input	Example
com.aris.umc.kerberos.servicePrincipalName	Principal Specifies the name of the user used for verifying Kerberos tickets. If Kerberos is used, each user, computer or service provided by a server must be defined as a principal.	String	MyLogin
com.aris.umc.kerberos.tenant	Default tenant Specifies the default tenant for a Kerberos-based login. Cross-tenant property that cannot be changed.	String	
com.aris.umc.kerberos.validateuser	Validate user name Specifies if the user name needs to be validated for separator. The default value is **false**.	true, false	
com.aris.umc.kerberos.allowlocalusers	Allow local users 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.	true, false	

6.3   Configure Single Sign-On using SAML

Single Sign-On with SAML can be used with applications running in a browser.

SAML is a standard for exchanging authentication data between security domains. SAML is an XML-based protocol that uses security tokens containing assertions to pass information about a user between an identity provider and a service provider and enables web-based authentication scenarios including single sign-on across all ARIS Connect runnables.

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.

- The SAML identity provider supports the HTTP POST binding as specified by the SAML 2.0 specification.

Client

Web browser supports JavaScript.

The following steps must be taken to use SSO:

Procedure

1. The Single Sign-On configuration options must be set in the ARIS Administration.

2. ARIS must be registered as a trusted service provider at the SAML identity provider.

You configured SSO.

CONFIGURATION OPTIONS IN ARIS ADMINISTRATION

You need to configure SSO for the servers.

Prerequisite

- 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.

Procedure

1. Log in to the ARIS Administration.
2. Click the arrow next to your name.
3. Click **Administration**.
4. Click **Configuration**.
5. Switch to **User management**.
6. Click the arrow next to **SAML**.
7. Click **General**.
8. Click ✎ **Edit**.
9. Enable **Use SAML**.
10. Enter the ID of the identity provider in the **Identity provider ID** field.
11. Enter the ID of the service provider in the **Service provider ID** field.
12. Enter the end point of the identity provider that is used for single sign-on in the **Single sign-on URL** field.
13. Enter the end point of the identity provider that is used for single log-out in in the **Single logout URL** field.

You have configures SSO using SAML in ARIS Administration. If you use multiple LDAP systems, the user names must be unambiguous through all LDAP systems. Otherwise no SSO is possible.

Please note that SSO (single sign-on) using SAML will not work in case of multiple LDAP servers and same login names (even with different entities) in different LDAP systems.

REGISTER ARIS AS A TRUSTED SERVICE PROVIDER

Establish a circle of trust between the identity provider and the service provider.

Procedure

1. Open a browser.
2. Enter the following URL in the address bar:

   `https://<SERVERNAME>/umc/rest/saml/metadata.xml?tenant=<TENANTID>`
3. iptables -t nat -A PREROUTING -i <network interface> -p tcp --dport <port n
4. Upload the file into your SAML identity provider.

Your system is configured to be used with Single Sign-On and SAML.

TROUBLESHOOTING

Detailed information on SAML authentication issues can be found in the log files of ARIS Administration located in

<Your installation folder>\ARIS9.8\server\bin\work\work_umcadmin_<size>\base\logs

Example

C:\SoftwareAG\ARIS9.8\server\bin\work\work_umcadmin_m\base\logs

6.4   SAML keys

You can configure SAML as required.

Key	Description	Valid input
com.aris.umc.saml.active	Use SAML Specifies whether an SAML-based login is allowed.	true, false
com.aris.umc.saml.binding	Binding 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**.	
com.aris.umc.saml.identity.provider.id	Identity provider ID Specifies the ID of the identity provider.	String
com.aris.umc.saml.service.provider.id	Service provider ID Specifies the ID of the service provider.	String
com.aris.umc.saml.identity.provider.sso.url	Single sign-on URL Specifies the end point of the identity provider that is used for single sign-on.	
com.aris.umc.saml.identity.provider.logout.url	Single logout URL Specifies the end point of the identity provider that is used for single log-out.	
com.aris.umc.saml.signature.assertion.active	Sign assertions 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.	true, false

Key	Description	Valid input
com.aris.umc.saml.signature.request.active	Sign requests 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.	true, false
com.aris.umc.saml.signature.response.active	Sign responses 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.	true, false
com.aris.umc.saml.signature.metadata.active	Sign metadata Enforces that the SAML metadata must be signed. If set, the service provider metadata file provided by the application is signed.	true, false
com.aris.umc.saml.signature.algorithm	Signature algorithm Specifies the algorithm for the signature. The algorithm can be selected from the list.	String
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.	String
com.aris.umc.saml.keystore.password	Password Specifies the password that is used to access the keystore.	String

Key	Description	Valid input
com.aris.umc.saml.keystore.typ yp	Type Specifies the type of the keystore to be used. The keystore type can be selected from a list.	String
com.aris.umc.saml.truststore .location	Truststore Specifies the location of the truststore file used for validating SAML assertions. The keystore must have been uploaded previously.	
com.aris.umc.saml.truststore .alias	Alias Specifies the alias to be used for accessing the truststore.	String
com.aris.umc.saml.truststore .password	Password Specifies the password to be used for accessing the truststore.	String
com.aris.umc.saml.truststore .type	Type Specifies the type of the truststore.	String
com.aris.umc.saml.login.mod e.dn.active	Login using DN Specifies whether login is to be tried using the fully qualified name instead of the user name.	true, false
com.aris.umc.saml.login.mod e.keyword.active	Decompose DN Specifies whether the fully qualified name is to be decomposed.	true, false
com.aris.umc.saml.login.mod e.keyword.name	Keyword Specifies which part of the fully qualified name is to be used for login.	String

Key	Description	Valid input
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**.	String
com.aris.umc.saml.auth.context.comparison	Authentication context comparison 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**.	String
com.aris.umc.saml.auth.nameid.format	NameID format Specifies in which format the user ID is transferred to ARIS Administration.	String
com.aris.umc.saml.login.users.create	Automatically create user 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 will apply to automatically created users: ▪ 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.	true, false

Key	Description	Valid input
com.aris.umc.saml.assertion.querystring	SAML assertion as a query string Defines whether or not the SAML assertion can be part of a query string. Cross-tenant property that cannot be changed.	true, false
com.aris.umc.saml.roles.extension	Include roles Specifies whether or not roles should be included. Cross-tenant property that cannot be changed.	true, false
com.aris.umc.saml.roles.attributeName	Attribute name for reading roles from assertion Defines the attribute name to be used to read roles from an SAML assertion. Cross-tenant property that cannot be changed.	String
com.aris.umc.saml.assertion.timeoffset	Clock skew Specifies the time offset between identity provider and service provider in seconds. Assertions are accepted if they are received within the permitted time frame.	
com.aris.umc.saml.assertion.ttl	Assertion lifetime Specifies the maximum lifetime of a SAML assertion in seconds.	
com.aris.umc.saml.tenant	Default tenant Specifies the default tenant that is to be used for the SAML-based login.	String

7 Disclaimer

ARIS products are intended and developed for use by persons. Automated processes, such as the generation of content and the import of objects/artifacts via interfaces, can lead to an outsized amount of data, and their execution may exceed processing capacities and physical limits. For example, processing capacities are exceeded if models and diagrams transcend the size of the modeling area or an extremely high number of processing operations is started simultaneously. Physical limits may be exceeded if the memory available is not sufficient for the execution of operations or the storage of data.

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

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

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

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

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

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