ARIS

SSO, SAML, LDAP, KERBEROS

VERSION 10.0 - SERVICE RELEASE 8

April 2019

This document applies to ARIS Version 10.0 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Contents

1 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 (for example, 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.

2 Customize 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.

To customize Kerberos, please refer to the ARIS Connect online help (see chapter **Administrate ARIS Connect > Configure ARIS Connect > Set up user management > Customize Kerberos settings**). If you are going to migrate data from ARIS 9.8.7 or later, customize Kerberos after the migration. The Kerberos settings of the former ARIS version will overwrite the current settings during data migration.

You can use Kerberos for single sign-on.

3 Customize 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.

To customize SAML, please refer to the ARIS Connect online help (see chapter **Administrate ARIS Connect > Configure ARIS Connect > Set up user management > Customize SAML**).

You can use SAML with single sign-on.

4 Use LDAP

4.1 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. Start ARIS Connect.
2. Click <user name> and select **Administration**.
3. Click **Configuration**.
4. Activate **User Management**.
5. Click the arrow next to **LDAP**.
6. Click **General settings**.
7. Click ✎ **Edit**.
8. Enable **Activate LDAP**.
9. Optional: Enable **Activate multiple LDAP integration**.
10. Click 💾 **Save**.
11. Click ✚ **Add**. The **Add LDAP server** dialog opens.
12. Enter the following:
    - 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

13. Specify the read timeout
14. 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.

4.2 Customize LDAP

To customize LDAP, please refer to the ARIS Connect online help (see chapter **Administrate ARIS Connect > Configure ARIS Connect > Set up user management > Customize LDAP settings**).

4.3 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. Start ARIS Connect.
2. Click <user name> and select **Administration**.
3. Click **Configuration**.
4. Click **User management**.
5. Click the arrow next to **LDAP**.
6. Click **General settings**.
7. Click **Edit**.
8. Enable **Activate LDAP**.
9. If you want to upload a configuration, ensure that you have disabled pop-up blockers in the browser.

   Click **Truststore**.
10. Click **Upload.** The **Truststore** dialog opens.
11. Select the relevant LDAP server.
12. Configure the URL for the LDAP system. Click **Connection**.
13. Enter an ID, a name, and the URL in the **Server URL** field, for example:
    `ldap://hqgc.mycompany.com:3168.`
14. 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.
15. Click **Behavior**.

16. Enter the Path to the user group in the **Group search paths** field.
17. 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.

4.4 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. Start ARIS Connect.
2. Click <user name> and select **Administration**.
3. Click **Configuration**.
4. Click **User management**.
5. Click the arrow next to **LDAP**.
6. Select 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://hqgc.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 **STARTTLS** 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.

SSL

Procedure

1. Start ARIS Connect.
2. Click <user name> and select **Administration**.
3. Click **Configuration**.
4. Click **User management**.
5. Click the arrow next to **LDAP**.
6. Select 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://hqgc.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

4.5 Configure single sign-on

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 for this.

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.

4.5.1 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. 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.

The following steps must be taken to use SSO:

Procedure

1. A technical user must be created in the Microsoft® Active Directory Domain Services.
2. A service principal name must be registered on the technical user.
3. The single sign-on configuration options must be set in 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 Domain Services. This user must be created in the Microsoft® Active Directory Domain Services 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 Domain Services without being prompted for a password. The most common use of keytab files is to allow scripts to authenticate against the Microsoft® Active Directory Domain Services 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 - for example **ktab –a aristechuser@MYDOMAIN.COM –n0 –append –k umc.keytab**.

CONFIGURATION IN ARIS ADMINISTRATION

You need to configure SSO for the servers.

Procedure

1. Start ARIS Connect.
2. Click <user name> and select **Administration**.
3. Click **Configuration**.
4. Click **User management**.
5. Click the arrow next to **Kerberos**.
6. 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
   ```
7. To upload the configuration file, click **Upload** under the **Configuration file** field.
8. Click **Edit**.
9. Enable **Use Kerberos**.
10. 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.
11. In the **Realm** field, configure the realm for the Kerberos service. Enter the fully qualified domain name in uppercase letters.

    Example: **MYDOMAIN.COM**.
12. In the **KDC** field, configure the fully qualified name of the KDC to be used.

13. **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 31).

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.

4.5.2 Kerberos keys

You can configure Kerberos as required.

Properties that are highlighted as cross-tenant properties can only be changes using ARIS Cloud Controller Command-line Tool. To change these 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	Valid input	Example
com.aris.umc.kerberos.active	**Use Kerberos** Specifies whether a Kerberos-based login is allowed.	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	mykdc.mydomain.com
com.aris.umc.kerberos.realm	**Realm** Specifies the realm of Kerberos tickets. Fully qualified domain name in uppercase letters.	String	MY.CORP.SOFTWAREAG.COM
com.aris.umc.kerberos.servicePrincipalName	**Principal** Specifies the name of the technical 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

Key	Description	Valid input	Example
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.config	**Configuration file** Storage location of the configuration file for Kerberos. The file can be uploaded directly.	String	./config/Kerberos/krb5.conf

ADVANCED SETTINGS

Key	Description	Valid input	Example
com.aris.umc.kerberos.debug	**Debug output** Specifies whether debug output is allowed for Kerberos operations.	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	
com.aris.umc.kerberos.validateuser	**Ignore realm from service ticket** 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**.	true, false	
com.aris.umc.kerberos.tenant	**Default tenant** Specifies the default tenant for a Kerberos-based login. Cross-tenant property that can only be changed using ARIS Cloud Controller. For further information, refer to **ARIS Cloud Controller (ACC) Command-line Tool manual**.	true, false	

4.5.3 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.

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

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

You only have access to the meta data XML file if SAML is enabled**.**

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 IN ARIS ADMINISTRATION

You need to configure SSO for the servers.

Prerequisite

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

Procedure

1. Start ARIS Connect.
2. Click <user name> and select **Administration**.
3. Click **Configuration**.
4. Click **User management**.
5. Click the arrow next to **SAML**.
6. Click **General**.
7. Click **Edit**.
8. Enable **Use SAML**.
9. Enter the ID of the identity provider in the **Identity provider ID** field.
10. Enter the ID of the service provider in the **Service provider ID** field.
11. Enter the end point of the identity provider that is used for single sign-on in the **Single sign-on URL** field.
12. 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 (page 31), the user names must be unambiguous through all LDAP systems. Otherwise no SSO is possible.

You can use SAML with multiple LDAP systems (page 31).

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 into 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>\ARIS10.0\server\bin\work\work_umcadmin_<size>\base\logs

Example

C:\SoftwareAG\ARIS10.0\server\bin\work\work_umcadmin_m\base\logs

4.5.4 SAML keys

You can configure SAML as required.

Properties that are highlighted as cross-tenant properties can only be changes using ARIS Cloud Controller Command-line Tool. To change these 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	Valid input	Example
com.aris.umc.saml.active	**Use SAML** Specifies whether an SAML-based login is allowed.	true, false	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**.		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	

Key	Description	Valid input	Example
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.		

SIGNATURE

Key	Description	Valid input	Example
com.aris.umc.saml.signature.assertion.active	**Enforce signing of 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	false
com.aris.umc.saml.signature.request.active	**Enforce signing of 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	false

Key	Description	Valid input	Example
com.aris.umc.saml.signature.response.active	**Enforce signing of 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	false
com.aris.umc.saml.signature.metadata.active	**Enforce signing of metadata** Enforces that the SAML metadata must be signed. If set, the service provider metadata file provided by the application is signed.	true, false	false
com.aris.umc.saml.signature.algorithm	**Signature algorithm** Specifies the algorithm for the signature. The algorithm can be selected from the list.	String	

KEYSTORE

Key	Description	Valid input	Example
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	
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.	String	JKB

TRUSTSTORE

Key	Description	Valid input	Example
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.	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	JKB

USER ATTRIBUTES

Key	Description	Valid input	Example
com.aris.umc.saml.attribute.fname	**First name** Specifies the attribute name to be used for reading first names from a SAML assertion.	String	John
com.aris.umc.saml.attribute.lname	**Last name** Specifies the attribute name to be used for reading last names from a SAML assertion.	String	Doe
com.aris.umc.saml.attribute.email	**E-mail address** Specifies the attribute name to be used for reading e-mail addresses from a SAML assertion.	String	jd@company.com
com.aris.umc.saml.attribute.phone	**Telephone number** Specifies the attribute name to be used for reading phone numbers from a SAML assertion.	Integer	01234567
com.aris.umc.saml.attribute.memberof	**Member of** Attribute that references the groups of a user.	String	Main group
com.aris.umc.saml.attribute.userdefined	**User-defined** Comma-separated list of attributes to be imported as user-defined attributes of the user.		

ADVANCED SETTINGS

Key	Description	Valid input	Example
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.	true, false	
com.aris.umc.saml.login.mode.keyword.active	**Decompose DN** Specifies whether the fully qualified name is to be decomposed.	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.	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**.	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	

Key	Description	Valid input	Example
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 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	false
com.aris.umc.saml.assertion.timeoffset	**Clock skew (in seconds)** Specifies the time offset between identity provider and service provider in seconds. Assertions are accepted if they are received within the permitted time frame.		60
com.aris.umc.saml.assertion.ttl	**Assertion lifetime (in seconds)** Specifies the maximum lifetime of a SAML assertion in seconds.		10

Key	Description	Valid input	Example
com.aris.umc.saml.service.provider.assertion.consumer.url.overwrite	**Assertion consumer service URL** 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/initsso**. If no specification is made, the URL is derived from the HTTP request.		
com.aris.umc.saml.tenant	**Default tenant** Specifies the default tenant that is to be used for the SAML-based login. Cross-tenant property that can only be changed using ARIS Cloud Controller. For further information, refer to **ARIS Cloud Controller (ACC) Command-line Tool manual**.	String	default

4.6 Use ARIS with multiple LDAP systems

ARIS supports the use of multiple LDAP systems (page 4). We strongly recommend that you contact your local Software AG sales organization (http://www.softwareag.com) before you start configuring multiple LDAP servers.

- If you are going to use multiple LDAP systems with already existing data, for example, attributes, all data must be renewed first.
- Each LDAP server must have a unique ID to identify the server to be used at user login and for user group names.
- The format of the ID must not exceed five characters
- The user or user group names are prefixed with the server ID in the following format: LDAP1\user1, LDAP2\user group name.

If the user name is defined in the format shown above, the users must enter the prefix when logging in.

4.6.1 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.

4.6.2 Use 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.

4.6.3 Single sign-on

If users have the same login ID in different LDAP servers, the Single sign-on (page 10) login fails. Users have to enter their passwords manually instead.

4.6.4 WebDAV

The WebDAV protocol provides a framework for users to create, change and move documents on a server. The most important features of the WebDAV protocol include the maintenance of properties about, for example, an author or modification date.

Using WebDAV with ARIS document storage works for local users only.

4.6.5 ARIS Architect

When using the search functionality in ARIS Architect, you must search for a user with his prefix.

Example

Search for a user in ARIS Architect for user **LDAP1\user1**, the user is found.

Search for user **user1** without the prefix, the user is not found.

4.6.6 Process Governance

All user names in all existing organizational charts must be updated with the prefix of the additional LDAP servers from which the users are imported.

5 Legal information

5.1 Documentation scope

The information provided describes the settings and features as they were at the time of publishing. Since documentation and software are subject to different production cycles, the description of settings and features may differ from actual settings and features. Information about discrepancies is provided in the Release Notes that accompany the product. Please read the Release Notes and take the information into account when installing, setting up, and using the product.

If you want to install technical and/or business system functions without Software AG's consulting services, you require extensive knowledge of the system to be installed, its intended purpose, the target systems, and their various dependencies. Due to the number of platforms and interdependent hardware and software configurations, we can only describe specific installations. It is not possible to document all settings and dependencies.

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

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

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

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

5.2 Data protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR).

Where applicable, appropriate steps are documented in the respective administration documentation.

5.3 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.

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

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

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

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

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

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