ARIS

SSO, SAML, LDAP, KERBEROS

Version 10.0 - Service Release 5

July 2018

Document content not changed since release 10.0.4. It applies to version 10.0.5 without changes.

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, for example, 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 (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.

3   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 the ⊞ **Configuration** tab.
4. Activate **User Management**.
5. Click the arrow next to **LDAP**.
6. Click **General settings**.
7. Click ✎ **Edit**.
8. Enable **Activate LDAP**.
9. 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   Customize LDAP settings

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**).

5 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 the ⊞ **Configuration** tab.

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.

You have configured ARIS for LDAP server operations.

6 Configure secure communication between ARIS and LDAP server

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 the **Configuration** tab.

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 the ⊞ **Configuration** tab.

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 mod**e 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

7 Use ARIS with multiple LDAP systems

ARIS supports the use of multiple LDAP systems (page 3). We strongly recommend that you contact your local Software AG sales organization (http://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.

7.1 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.

7.2 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.

7.3 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.

7.4 WebDAV

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

7.5   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.

7.6   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.

8 Configure single sign-on

If you are using MS 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 MS Active Directory Domain Services.

- The browser used supports a Kerberos-based authentication.

- The browser has been configured accordingly.

CONFIGURATION IN ARIS ADMINISTRATION USING KERBEROS

SSO must be configured for the servers.

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.

Prerequisite

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

Procedure

1. Start ARIS Connect.

2. Click <user name> and select **Administration**.

3. Click the 🔲 **Configuration** tab.

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 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.

CONFIGURATION IN ARIS ADMINISTRATION USING SAML

SSO must be configured 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. Start ARIS Connect.

2. Click <user name> and select **Administration**.

3. Click the **Configuration** tab.

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, 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.

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.

9 Customize Kerberos settings

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. While migrating data, the Kerberos settings of the former ARIS version will overwrite the current settings.

10 Customize SAML

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**).

11   Disclaimer

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

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

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

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

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

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

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