# ARIS

# SSO, SAML, LDAP, KERBEROS

Version 10.0 - Service Release 1

**July 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 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**).

# 4 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 your user name and select **Administration**.
3. Activate the **Configuration** tab.
4. Click **User management**.
5. Select **LDAP** in the list box.
6. Click **Connection**.
7. Click **Edit**.
8. Enable **Activate LDAP**.

   If you want to upload a configuration, ensure that pop-up blockers are disabled in the browser, and click the field next to the relevant key.

   The dialog for selecting the file opens.
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, if this backup system is used for your LDAP system and automatically applies the function of the original system, if required in the **Server URL (fallback)** field.

    Click **Behavior**.
11. Enter the Path to the user group in the **Group search paths** field.
12. Enter the Path to the users in the **User search paths** field.

    If you want to enable the function of following referrals of users to other directories, enter **follow** in the **Referral** field.

    If you want to avoid the above behavior, enter **ignore** in the **Referral** field.

    If you leave this entry blank, referrals are not followed.

    Optional: If you want to ensure that the import of LDAP users is carried out despite any errors that might occur, e.g., if names are redundant, click **Advanced settings** and enable **Skip errors**.

    Please note that system performance is significantly deteriorated if you enable this option.

# 5 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 your user name and select **Administration**.
3. Activate the **Configuration** tab.
4. Click **User management**.
5. Select **LDAP** in the list box.
6. Click **Connection**.
7. Click **Edit**.
8. Configure the URL for the LDAP system. To do so, enter the URL as in the **Server URL** field, for example:
   **`ldap://hqgc.mycompany.com:3168`**.
9. Configure the path to the backup system, if this backup system is used for your LDAP system and automatically applies the function of the original system, if required in the **Server URL (fallback)** field.
10. Enable **Use SSL**.
11. Select **STARTTLS** from the **SSL mode** list.
12. ARIS must trust the LDAP server used. Therefore, we recommend that you use the LDAP server with a certificate signed by a public certification authority. If your certificate is signed by a public certification authority and stored in the list of trustworthy certificates of your JRE, you do not need to configure anything else.
13. Upload LDAP truststore file.

You can upload the truststore file.

### Prerequisite

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

### Procedure

1. Start ARIS Connect.
2. Click your user name and select **Administration**.
3. Activate the **Configuration** tab.
4. Activate **User Management**.
5. Select **LDAP** in the list box.
6. Click **Truststore**.
7. Click **Upload > Truststore**. The dialog for uploading a file opens.
8. Select the relevant file.

You have uploaded a truststore file.

## SSL

### Procedure

1. Start ARIS Connect.
2. Click your user name and select **Administration**.
3. Activate the **Configuration** tab.
4. Click **User management**.
5. Select **LDAP** in the list box.
6. Click **Connection**.
7. Click **Edit**.
8. Configure the URL for the LDAP system. To do so, enter the URL as in the **Server URL** field, for example:
   **`ldap://hqgc.mycompany.com:3168`**.
9. Configure the path to the backup system, if this backup system is used for your LDAP system and automatically applies the function of the original system, if required in the **Server URL (fallback)** field.
10. Enable **Use SSL**.
11. Select **SSL** from the **SSL mod**e list.
12. ARIS must trust the LDAP server used. Therefore, we recommend that you use the LDAP server with a certificate signed by a public certification authority. If your certificate is signed by a public certification authority and stored in the list of trustworthy certificates of your JRE, you do not need to configure anything else.
13. Upload LDAP truststore file

You can upload the truststore file.

### Prerequisite

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

### Procedure

1. Start ARIS Connect.
2. Click your user name and select **Administration**.
3. Activate the **Configuration** tab.
4. Activate **User Management**.
5. Select **LDAP** in the list box.
6. Click **Truststore**.
7. Click **Upload > Truststore**. The dialog for uploading a file opens.
8. Select the relevant file.

You have uploaded a truststore file.

# 6 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.

Single sign-on in ARIS is based on 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 MS Windows networks. In addition, it is widely used with Linux operating systems and is designed for use with all major platforms.

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 a Kerberos-based authentication (default) and the Service Principal Name of the ARIS Server has the following format: **HTTP/<host name>**, e.g., **HTTP/mypc01.my.domain.com**.

**Client**

- Client and server computers are connected with to the same MS Active Directory Domain Services.
- The browser used supports Kerberos-based authentication.
- The browser used has been configured accordingly.

## CONFIGURATION IN ARIS ADMINISTRATION USING KERBEROS

SSO must be configured for the servers.

### Prerequisite

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

### Procedure

1. Start ARIS Connect.
2. Click your user name and select **Administration**.
3. Activate the **Configuration** tab.
4. Click **User management**.
5. Select **Kerberos** in the list box.

   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
   ```
6. Click **Import configuration file**.
7. Click **Edit**.
8. Enable **Use Kerberos**.
9. In the **Principal** field, enter the technical user name given by the administrator.

   If the Service Principal Name in the keytab is, for example, **mypc01@MY.DOMAIN.COM**, the values of the property **com.company.aris.umc.kerberos.servicePrincipalName** must contain the Service Principal Name exactly as specified in the keytab file.
10. In the **Realm** field, configure the realm for the Kerberos service. Enter the fully qualified domain name in uppercase letters.

    Example: **MYDOMAIN.COM**.
11. In the **KDC** field, configure the fully qualified name of the KDC to be used.
12. **Optional:**
    a. Click **Advanced settings**.
    b. Enable **Debug output**.

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

## CONFIGURATION IN ARIS ADMINISTRATION USING SAML

SSO must be configured for the servers.

### Prerequisite

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

### Procedure

1. Start ARIS Connect.
2. Click your user name and select **Administration**.
3. Activate the **Configuration** tab.
4. Click **User management**.
5. Select **SAML** in the list box.
6. Click **Edit**.
7. Enable **Use SAML**.
8. Enter the ID of the identity provider in the **Identity provider ID** field.
9. Enter the ID of the service provider in the **Service provider ID** field.
10. Enter the end point of the identity provider that is used for single sign-on in the **Single sign-on URL** field.
11. Enter the end point of the identity provider that is used for single log-out in in the **Single logout URL** field.

## 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.

# 7 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**).

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