ARIS

ARIS SSO - LDAP - KERBEROS - SAML - SCIM

VERSION 10.0 - SERVICE RELEASE 20 AND HIGHER

OCTOBER 2022

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

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

Copyright © 2010 - 2022 Software AG, Darmstadt, Germany and/or Software AG USA Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

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

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

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

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

Contents

Contents I

1 Choose your installation scenario 1

2 Set up LDAP (on-premises) 3
- 2.1 Overview 3
- 2.2 Procedure 4
- 2.3 Customize ARIS for LDAP server operations 8
- 2.4 Configure secure communication 10
- 2.5 Use ARIS with multiple LDAP systems 13
- 2.6 Set up SSO for LDAP with Kerberos 15
  - 2.6.1 Overview 15
  - 2.6.2 Procedure 16
- 2.7 Set up SSO for LDAP with SAML 17
  - 2.7.1 Overview 17
  - 2.7.2 Procedure 18

3 Set up LDAP (ARIS Enterprise) 21
- 3.1 Overview 21
- 3.2 Procedure 22
- 3.3 Customize ARIS for LDAP server operations 29
- 3.4 Configure secure communication 31
- 3.5 Use ARIS with multiple LDAP systems 34
- 3.6 Set up SSO for LDAP with SAML 35
  - 3.6.1 Overview 36
  - 3.6.2 Procedure 37

4 Set up SCIM (ARIS Enterprise) 40
- 4.1 Overview 40
- 4.2 Procedure 41
- 4.3 Set up SSO for SCIM with SAML 42
  - 4.3.1 Overview 42
  - 4.3.2 Procedure 43

5 Set up SCIM (ARIS Advanced Base Extension)) 46
- 5.1 Overview 46
- 5.2 Procedure 47
- 5.3 Set up SSO for SCIM with SAML 48
  - 5.3.1 Overview 48
  - 5.3.2 Procedure 49

6 Legal information 52
- 6.1 Documentation scope 52
- 6.2 Support 53

1 Choose your installation scenario

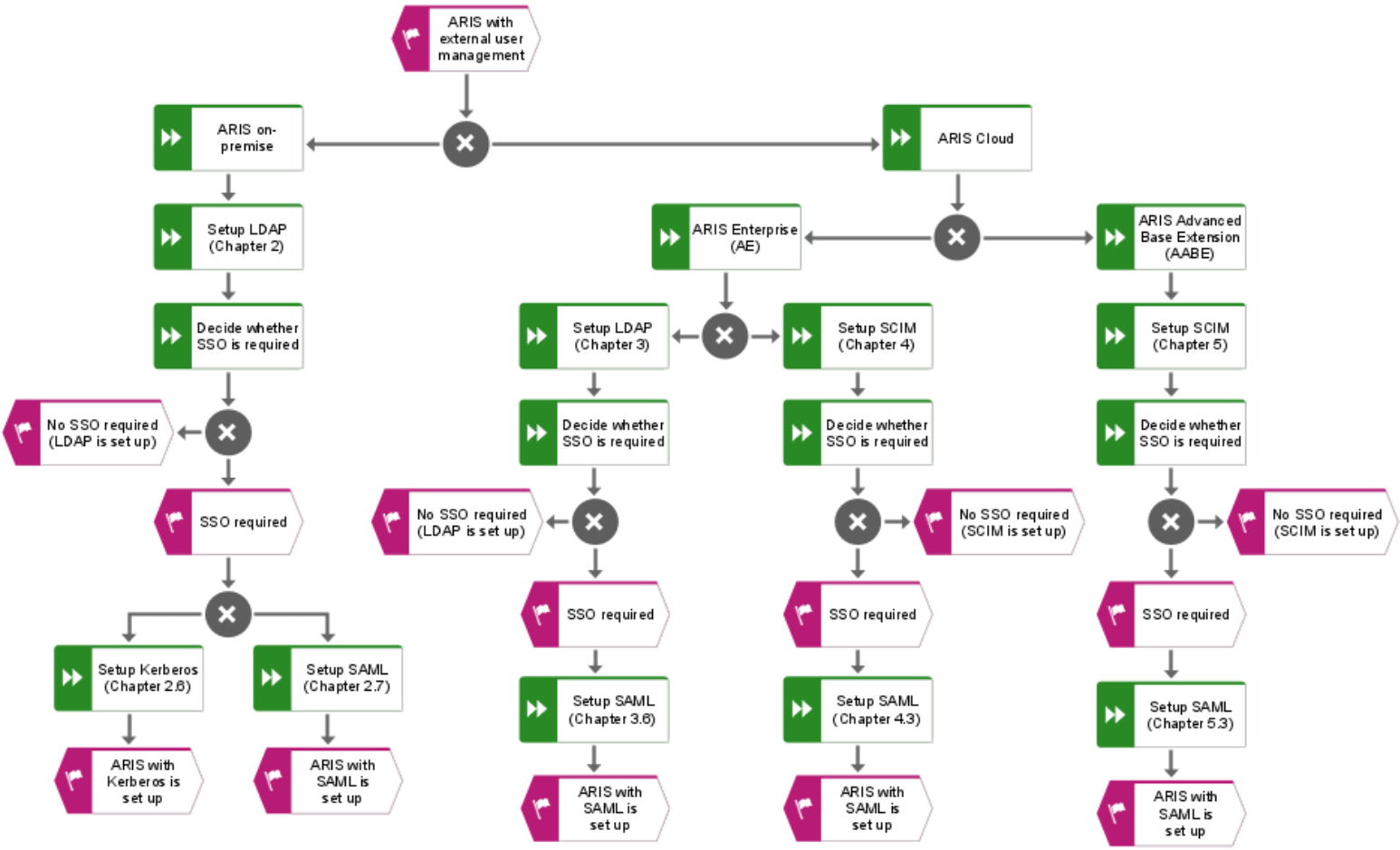
The following EPC shows the installation scenarios for LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) for on-premises products or SCIM (**S**ystem for **C**ross-domain **I**dentity **M**anagement) for cloud products. To use single sign-on, you must configure the appropriate authentication service (Kerberos) or protocol (SAML).

In the following model, you should follow the model path that reflects your system environment.

Example

If you want to establish ARIS on-premises with LDAP and SSO using SAML, use the following model path.

ARIS with external user management > **ARIS on-premises** > **Setup LDAP** > **Decide whether SSO is required** > **SSO required** > **Setup SAML**.



You can use ARIS on-premises together with an LDAP server (page 4).

You can use ARIS Enterprise (AE) together with an LDAP server (page 22) or a SCIM server (page 41).

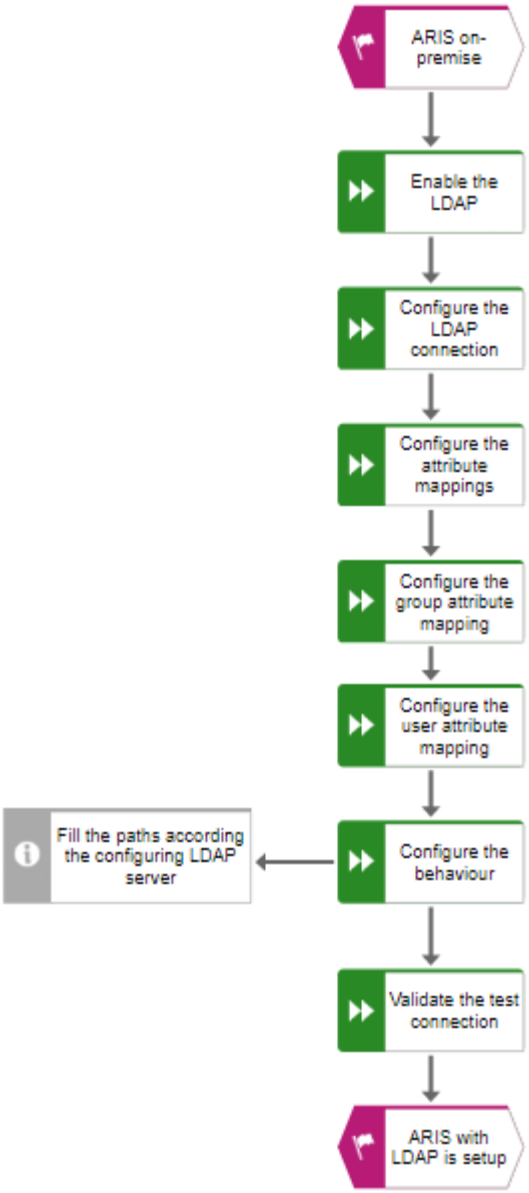
You can use single sign-on (SSO). The configuration of SSO is described in the following chapters depending on your installation:

- ARIS on-premises using LDAP with Kerberos (page 16)
- ARIS on-premises using LDAP with SAML (page 18)
- ARIS Enterprise (AE) using LDAP with SAML (page 37)
- ARIS Enterprise (AE) using SCIM with SAML (page 43)
- ARIS Advanced Base Extension (AABE) using SCIM with SAML (page 49)

2 Set up LDAP (on-premises)

LDAP stands for **L**ightweight **D**irectory **A**ccess **P**rotocol. This is an application protocol from network technology. LDAP enables information from a distributed, location-independent, and hierarchical database in a network to be queried and modified.

2.1 Overview



2.2 Procedure

Prerequisite

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

ENABLE LDAP

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User Management**.
4. Click the arrow next to **LDAP**.
5. Click **General settings**.
6. Click **Edit**.
7. Enable **Use LDAP**.
8. If you want to use ARIS with multiple LDAP systems, enable (page 13) **Activate multiple LDAP integration** and click **OK** in the **Confirmation of property value change** dialog.
9. Click **Save**.

You have added an LDAP server.

CONFIGURE THE LDAP CONNECTION.

1. Click + **Add**. The **Add LDAP server** dialog opens.
2. 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 to use SSL and in which mode.
   - Specify whether to verify host names and certificates.
   - Simultaneous connections are a cross-tenant property. You can change them only using ARIS Cloud Controller. For more information, refer to **ARIS Cloud Controller (ACC) Command-line Tool manual**.
   - Specify the connection timeout
   - Specify the read timeout
3. Click **Save**.

CONFIGURE THE ATTRIBUTE MAPPING

1. Click the arrow next to the relevant LDAP server.
2. Click **Attribute mappings**.
3. Click **Edit**.
4. Specify the attribute **objectClass**.
5. Specify the attribute **DN** that contains the fully qualified name (distinguishedName).
6. Specify the attribute **GUID** that contains the objectGUID.
7. Click **Save**.

CONFIGURE THE GROUP ATTRIBUTE MAPPING

1. Click the arrow next to the relevant LDAP server.
2. Click **Group attribute mappings**.
3. Click **Edit**.
4. Specify the attribute that contains the group name.
5. Specify the attribute that references the members of a group.
6. Specify a comma-separated list of LDAP attributes that are to be imported as user-defined attributes of a user group.
7. Click **Save**.

CONFIGURE THE USER ATTRIBUTE MAPPING

1. Click the arrow next to the relevant LDAP server.
2. Click **User attribute mapping**.
3. Click **Edit**.
4. Specify the attributes that contain the user attribute, for example, the first name, the last name, and the telephone number.
5. Click **Save**.

CONFIGURE THE BEHAVIOR OF LDAP

1. Click the arrow next to the relevant LDAP server.
2. Click **Behavior**.
3. Click **Edit**.
4. Specify the options you want to set:
   - the group and user object classes.
   - the search paths.
   - the search filters.
   - the recursion depth.
   - the page size.
   - the referrals.
5. Click **Save**.

TEST THE LDAP CONNECTION

1. Click the arrow next to the relevant LDAP server.
2. Click **Connection**.
3. Click **Test connection**.

If the LDAP connection is valid, ARIS with LDAP is set up.

If you want to use single sign-on, you can use Kerberos (page 16) or SAML 2.0 (page 18).

2.3 Customize ARIS for LDAP server operations

The LDAP server operations are used, for example,

- to import users or user groups and their members, or
- to preview users or user groups, or
- to synchronize users or user groups.

The preview is used to verify that the specified search paths and filters return the correct set of users or user groups.

The import imports the users or user groups and their members into ARIS.

When the users are imported into ARIS and a user or user group is changed on the LDAP server, you can synchronize to apply the latest changes to ARIS.

Prerequisite

- You have the **Technical configuration administrator** function privilege.
- You must have an already generated truststore file.

Procedure

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User management**.
4. Click the arrow next to **LDAP**.
5. Click **General settings**.
6. Click **Edit**.
7. Enable **Use LDAP**.
8. Click **Save**.
9. Click **Truststore**.
10. Click **Upload.** The **Truststore** dialog opens. Select the truststore file you want to use and click **Upload**.
11. Click the arrow next to the relevant LDAP server.
12. Click **Connection**.
13. Click **Edit**.
14. Configure the LDAP URL by entering an ID, a name, and the URL in the **Server URL** field, for example:

    `ldap://hqgc.mycompany.com:3168`.

15. Configure the fallback URL of the LDAP 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.
16. Click **Save**.
17. Click **Behavior**.
18. Click **Edit**.
19. Enter the path to the user group in the **Group search paths** field.
20. Enter the path to the users in the **User search paths** field.
21. If you configure only one LDAP server, you can skip this step.

    If you use a system with multiple LDAP servers (page 13), you must configure referrals.

    Select **ignore** if you do not want to search all configured LDAP servers. The LDAP operations are performed only on the primary LDAP server.

    Select **follow** if you want to execute the operations on all configured LDAP servers.

    Select **throw** if you want to execute the operations on all configured LDAP servers. All valid users are included, and the result is logged. Valid users and invalid users are listed in the **LDAP.log** file.
22. Click **Save**.

    To ensure that the import of LDAP users does not fail despite any errors that might occur, for example, if names are duplicated, click **LDAP > General settings > Advanced settings** and enable **Skip errors**.

You have configured ARIS for LDAP server operations.

2.4 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 LDAP is activated.
- ARIS Administration trusts the LDAP server. That means, the SSL certificate of the LDAP server or the certification authority is stored in the JRE database of trustworthy certificates.
- ARIS trusts the LDAP server. 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.

STARTTLS

You can use STARTTLS to configure encrypted communication between ARIS and the LDAP server.

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User management**.
4. Click the arrow next to **LDAP**.
5. Click the arrow next to the relevant LDAP server.
6. Click **Connection**.
7. Click **Edit**.
8. Configure the URL for the LDAP system. To do so, enter the URL as in the **Server URL** field, for example:

   `ldap://hqgc.mycompany.com:3168`.
9. Configure the fallback URL of the LDAP backup system in the **Server URL (fallback)** field. This backup system takes over automatically if the LDAP server cannot be reached via its primary URL.
10. Enable **Use SSL**.
11. Select **STARTTLS** from the **SSL mode** list.
12. Click **Save**.
13. Upload the LDAP truststore file (page 8).

SSL

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User management**.
4. Click the arrow next to **LDAP**.
5. Click the arrow next to the relevant LDAP server.
6. Click **Connection**.
7. Click **Edit**.
8. Configure the URL for the LDAP system. To do so, enter the URL as in the **Server URL** field, for example:

   `ldap://hqgc.mycompany.com:3168`.
9. Configure the fallback URL of the LDAP backup system in the **Server URL (fallback)** field. This backup system takes over automatically if the LDAP server cannot be reached via its primary URL.
10. Enable **Use SSL**.
11. Select **SSL** from the **SSL mode** list.
12. Click **Save**.
13. Upload the LDAP truststore file (page 8)

2.5 Use ARIS with multiple LDAP systems

ARIS supports the use of multiple LDAP systems.

Warning

The migration to multiple LDAP servers is irreversible. Any existing LDAP data needs to be deleted manually before the migration.

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 plan 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.

SINGLE SIGN-ON

If users have the same login ID in different LDAP servers, the single sign-on login fails. Users must enter their passwords manually instead.

KERBEROS

Even if you have configured multiple LDAP systems, you can use only one LDAP server with Kerberos authentication.

When you use multiple LDAP systems, you must enable the **Ignore realm from service ticket** property under **Kerberos > Advanced Settings**.

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.

WEBDAV

The WebDAV protocol provides a framework for users to create, change, and move documents on a server. The WebDAV protocol enables you to maintain properties related to, for example, an author or modification date.

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

ARIS ARCHITECT

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

Example

If you search for user LDAP1/user 1, the user is found.

If you search for user 1, the user is not found.

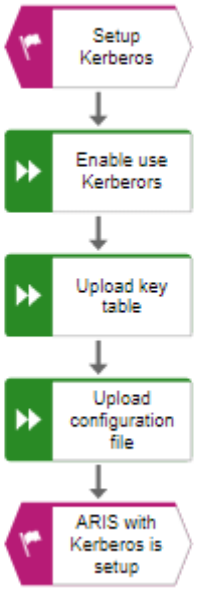
PROCESS GOVERNANCE

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

2.6 Set up SSO for LDAP with Kerberos

Kerberos is a distributed authentication service for open and non-secure computer networks. With ARIS in 10.0 from service release 18 on and with the upgrade to JRE 17, the Triple Data Encryption Algorithm (Triple-DES or 3DES) and the Rivest Cipher 4 (RC4) as symmetric-key-algorithms for the encryption of digital data are no longer supported because these algorithms are considered as too insecure for modern applications.

2.6.1 Overview



2.6.2 Procedure

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.

ENABLE SSO FOR THE SERVERS (KERBEROS)

1. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
2. Click **User Management**.
3. Click the arrow next to **Kerberos**.
4. Click **General**.
5. Click **Edit**.
6. Enable **Use Kerberos**.
7. Click **Save**.

You have enabled Kerberos.

UPLOAD A KEY TABLE

To upload the key table file, click **Upload** under the **Key table** field.

You can display the content of an existing key table file using the JRE tool **ktab.exe**. To do so, enter the following command on the command line:

```
ktab -l -e -t -k FILE:C:\<file location of the umc.ktab file>\umc.ktab
```

If you have no key table file available, generate a key table file using the JRE tool **ktab.exe**. To do so, enter the following command on the command line:

```
ktab -a userPrincipalName@REALM password -n 0 -append -k umc.keytab
```

UPLOAD A CONFIGURATION FILE

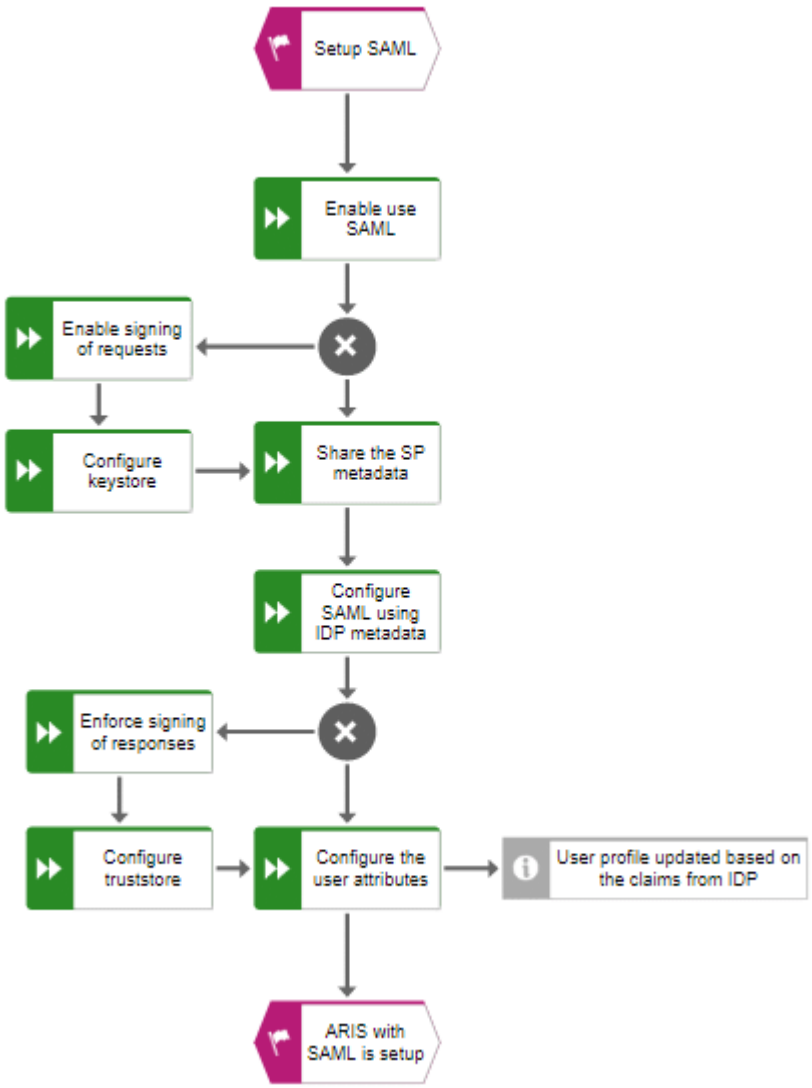
1. To upload the configuration file, click **Upload** under the **Configuration file** field. You find this file on your installation medium under **Add-ons\Kerberos**. The dialog for uploading a file opens.
2. Select the relevant file and click **Upload**.

You have uploaded a configuration file.

2.7 Set up SSO for LDAP with SAML

SAML (**S**ecurity **A**ssertion **M**arkup **L**anguage) 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 it enables web-based authentication scenarios including single sign-on across all ARIS runnables.

2.7.1 Overview



2.7.2 Procedure

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 metadata XML file if SAML is enabled.
- ARIS must be registered as a trusted service provider at the SAML identity provider.

Client

Your web browser supports JavaScript.

ENABLE SSO FOR THE SERVERS (SAML)

Prerequisite

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

Procedure

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User management**.
4. Click the arrow next to **SAML**.
5. Click **General**.
6. Click **Edit**.
7. Enable **Use SAML**.
8. Enter the ID of the identity provider in the **Identity provider ID** field.
9. Enter the ID of the service provider in the **Service provider ID** field, for example **UMC@<server name>**.
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.
12. Click **Save**.

OPTIONAL SAML SETTINGS

1. Click **Signature**.
2. Click **Edit**.
3. Enable the check box of the options you want to set:
   - Enforce signing of assertions
   - Enforce signing of requests
   - Enforce signing of responses
   - Enforce signing of metadata
   - Select signature algorithm
4. Click **Save**.

You have enabled the signing. If you have enabled this option, you must configure the truststore.

OPTIONAL: CONFIGURE THE KEYSTORE

1. Click **Keystore**.
2. Click **Upload**. The dialog opens. Select the keystore file on your file system and click **Upload**.
3. Click **Edit**.
4. Configure your keystore.
5. Click **Save**.

You have configured the keystore.

SHARE THE SERVICE PROVIDER (SP) METADATA

1. Click **General**.
2. Send the service provider ID to your identity provider (IDP).

CONFIGURE SAML USING IDENTITY PROVIDER (IDP) METADATA

1. Click **General**.
2. Click **Edit**.
3. Enter the identity provider ID.
4. Click **Save**.

OPTIONAL: CONFIGURE THE TRUSTSTORE

1. Click **Truststore**.
2. Click **Upload**. The dialog opens. Select the truststore file on your file system and click **Upload**.
3. Click **Edit**.
4. Configure your truststore.
5. Click **Save**.

You have configured the truststore.

CONFIGURE THE USER ATTRIBUTES

1. Click **User attributes**.
2. Click **Edit**.
3. Specify the attribute fields, for example, the first name, the last name, or the e-mail.
4. Click **Save**.

You have configured the user attributes.

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>`

   You get a metadata file. Save this file as an XML file.
3. Send the metadata file to your SAML identity provider that the metadata can be uploaded.

Your system is configured to be used with single sign-on and SAML.

TROUBLESHOOTING

You can find detailed information on SAML authentication issues in the log files of ARIS Administration located in

```
<Your installation
folder>\ARIS10.0\server\bin\work\work_umcadmin_<size>\base\logs
```

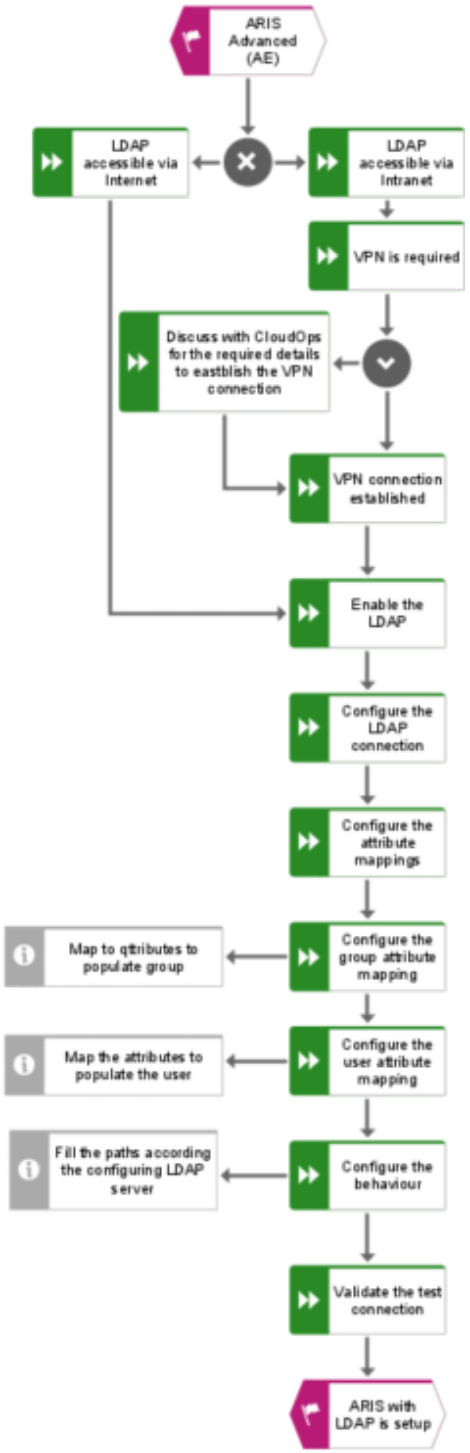
Example

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

3 Set up LDAP (ARIS Enterprise)

LDAP stands for **L**ightweight **D**irectory **A**ccess **P**rotocol. This is an application protocol from network technology. LDAP enables information from a distributed, location-independent, and hierarchical database in a network to be queried and modified.

3.1 Overview



3.2 Procedure

Prerequisite

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

LDAP ACCESSIBLE VIA INTERNET

If your LDAP server is accessible via the Internet, proceed as follows.

ENABLE LDAP

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User Management**.
4. Click the arrow next to **LDAP**.
5. Click **General settings**.
6. Click **Edit**.
7. Enable **Use LDAP**.
8. If you want to use ARIS with multiple LDAP systems, enable (page 13) **Activate multiple LDAP integration** and click **OK** in the **Confirmation of property value change** dialog.
9. Click **Save**.

You have added an LDAP server.

CONFIGURE THE LDAP CONNECTION.

1. Click + **Add**. The **Add LDAP server** dialog opens.
2. 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 to use SSL and in which mode.
   - Specify whether to verify host names and certificates.
   - Simultaneous connections are a cross-tenant property. You can change them only using ARIS Cloud Controller. For more information, refer to **ARIS Cloud Controller (ACC) Command-line Tool manual**.
   - Specify the connection timeout
   - Specify the read timeout
3. Click **Save**.

CONFIGURE THE ATTRIBUTE MAPPING

1. Click the arrow next to the relevant LDAP server.
2. Click **Attribute mappings**.
3. Click **Edit**.
4. Specify the attribute **objectClass**.
5. Specify the attribute **DN** that contains the fully qualified name (distinguishedName).
6. Specify the attribute **GUID** that contains the objectGUID.
7. Click **Save**.

CONFIGURE THE GROUP ATTRIBUTE MAPPING

1. Click the arrow next to the relevant LDAP server.
2. Click **Group attribute mappings**.
3. Click **Edit**.
4. Specify the attribute that contains the group name.
5. Specify the attribute that references the members of a group.
6. Specify a comma-separated list of LDAP attributes that are to be imported as user-defined attributes of a user group.
7. Click **Save**.

CONFIGURE THE USER ATTRIBUTE MAPPING

1. Click the arrow next to the relevant LDAP server.
2. Click **User attribute mapping**.
3. Click **Edit**.
4. Specify the attributes that contain the user attribute, for example, the first name, the last name, and the telephone number.
5. Click **Save**.

CONFIGURE THE BEHAVIOR

1. Click the arrow next to the relevant LDAP server.
2. Click **Behavior**.
3. Click **Edit**.
4. Specify the options you want to set:
   - the group and user object classes.
   - the search paths.
   - the search filters.
   - the recursion depth.
   - the page size.
   - the referrals.
5. Click **Save**.

TEST THE LDAP CONNECTION.

1. Click the arrow next to the relevant LDAP server.
2. Click **Connection**.
3. Click **Test connection**.

If the LDAP connection is valid, ARIS with LDAP is set up.

If you want to use single sign-on, you can use SAML 2.0 (page 18).

LDAP ACCESSIBLE VIA INTRANET

If you are using LDAP within the Intranet, you must establish VPN.

VPN stands for **v**irtual **p**rivate **n**etwork. VPN extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

VPN IS REQUIRED

1. Contact Cloud Operations (CloudOps) for the required details to establish a VPN connection.
2. Establish a VPN connection.

ENABLE LDAP

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User Management**.
4. Click the arrow next to **LDAP**.
5. Click **General settings**.
6. Click **Edit**.
7. Enable **Use LDAP**.
8. If you want to use ARIS with multiple LDAP systems, enable (page 13) **Activate multiple LDAP integration** and click **OK** in the **Confirmation of property value change** dialog.
9. Click **Save**.

You have added an LDAP server.

CONFIGURE THE LDAP CONNECTION.

1. Click + **Add**. The **Add LDAP server** dialog opens.
2. 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 to use SSL and in which mode.
   - Specify whether to verify host names and certificates.
   - Simultaneous connections are a cross-tenant property. You can change them only using ARIS Cloud Controller. For more information, refer to **ARIS Cloud Controller (ACC) Command-line Tool manual**.
   - Specify the connection timeout
   - Specify the read timeout
3. Click **Save**.

CONFIGURE THE ATTRIBUTE MAPPING

1. Click the arrow next to the relevant LDAP server.
2. Click **Attribute mappings**.
3. Click **Edit**.
4. Specify the attribute **objectClass**.
5. Specify the attribute **DN** that contains the fully qualified name (distinguishedName).
6. Specify the attribute **GUID** that contains the objectGUID.
7. Click **Save**.

CONFIGURE THE GROUP ATTRIBUTE MAPPING

1. Click the arrow next to the relevant LDAP server.
2. Click **Group attribute mappings**.
3. Click **Edit**.
4. Specify the attribute that contains the group name.
5. Specify the attribute that references the members of a group.
6. Specify a comma-separated list of LDAP attributes that are to be imported as user-defined attributes of a user group.
7. Click **Save**.

CONFIGURE THE USER ATTRIBUTE MAPPING

1. Click the arrow next to the relevant LDAP server.
2. Click **User attribute mapping**.
3. Click **Edit**.
4. Specify the attributes that contain the user attribute, for example, the first name, the last name, and the telephone number.
5. Click **Save**.

CONFIGURE THE BEHAVIOR

1. Click the arrow next to the relevant LDAP server.
2. Click **Behavior**.
3. Click **Edit**.
4. Specify the options you want to set:
   - the group and user object classes.
   - the search paths.
   - the search filters.
   - the recursion depth.
   - the page size.
   - the referrals.
5. Click **Save**.

TEST THE LDAP CONNECTION.

1. Click the arrow next to the relevant LDAP server.
2. Click **Connection**.
3. Click **Test connection**.

If the LDAP connection is valid, ARIS with LDAP is set up.

If you want to use single sign-on, you can use SAML 2.0 (page 18).

3.3 Customize ARIS for LDAP server operations

The LDAP server operations are used, for example,

- to import users or user groups and their members, or
- to preview users or user groups, or
- to synchronize users or user groups.

The preview is used to verify that the specified search paths and filters return the correct set of users or user groups.

The import imports the users or user groups and their members into ARIS.

When the users are imported into ARIS and a user or user group is changed on the LDAP server, you can synchronize to apply the latest changes to ARIS.

Prerequisite

- You have the **Technical configuration administrator** function privilege.
- You must have an already generated truststore file.

Procedure

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User management**.
4. Click the arrow next to **LDAP**.
5. Click **General settings**.
6. Click **Edit**.
7. Enable **Use LDAP**.
8. Click **Save**.
9. Click **Truststore**.
10. Click **Upload.** The **Truststore** dialog opens. Select the truststore file you want to use and click **Upload**.
11. Click the arrow next to the relevant LDAP server.
12. Click **Connection**.
13. Click **Edit**.
14. Configure the LDAP URL by entering an ID, a name, and the URL in the **Server URL** field, for example:

    `ldap://hqgc.mycompany.com:3168`.

15. Configure the fallback URL of the LDAP 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.
16. Click **Save**.
17. Click **Behavior**.
18. Click **Edit**.
19. Enter the path to the user group in the **Group search paths** field.
20. Enter the path to the users in the **User search paths** field.
21. If you configure only one LDAP server, you can skip this step.

    If you use a system with multiple LDAP servers (page 13), you must configure referrals.

    Select **ignore** if you do not want to search all configured LDAP servers. The LDAP operations are performed only on the primary LDAP server.

    Select **follow** if you want to execute the operations on all configured LDAP servers.

    Select **throw** if you want to execute the operations on all configured LDAP servers. All valid users are included, and the result is logged. Valid users and invalid users are listed in the **LDAP.log** file.
22. Click **Save**.

    To ensure that the import of LDAP users does not fail despite any errors that might occur, for example, if names are duplicated, click **LDAP > General settings > Advanced settings** and enable **Skip errors**.

You have configured ARIS for LDAP server operations.

3.4 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 LDAP is activated.
- ARIS Administration trusts the LDAP server. That means, the SSL certificate of the LDAP server or the certification authority is stored in the JRE database of trustworthy certificates.
- ARIS trusts the LDAP server. 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.

STARTTLS

You can use STARTTLS to configure encrypted communication between ARIS and the LDAP server.

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User management**.
4. Click the arrow next to **LDAP**.
5. Click the arrow next to the relevant LDAP server.
6. Click **Connection**.
7. Click **Edit**.
8. Configure the URL for the LDAP system. To do so, enter the URL as in the **Server URL** field, for example:

   `ldap://hqgc.mycompany.com:3168`.
9. Configure the fallback URL of the LDAP backup system in the **Server URL (fallback)** field. This backup system takes over automatically if the LDAP server cannot be reached via its primary URL.
10. Enable **Use SSL**.
11. Select **STARTTLS** from the **SSL mode** list.
12. Click **Save**.
13. Upload the LDAP truststore file (page 8).

SSL

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User management**.
4. Click the arrow next to **LDAP**.
5. Click the arrow next to the relevant LDAP server.
6. Click **Connection**.
7. Click **Edit**.
8. Configure the URL for the LDAP system. To do so, enter the URL as in the **Server URL** field, for example:

   `ldap://hqgc.mycompany.com:3168`.
9. Configure the fallback URL of the LDAP backup system in the **Server URL (fallback)** field. This backup system takes over automatically if the LDAP server cannot be reached via its primary URL.
10. Enable **Use SSL**.
11. Select **SSL** from the **SSL mode** list.
12. Click **Save**.
13. Upload the LDAP truststore file (page 8)

3.5 Use ARIS with multiple LDAP systems

ARIS supports the use of multiple LDAP systems.

Warning

The migration to multiple LDAP servers is irreversible. Any existing LDAP data needs to be deleted manually before the migration.

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 plan 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.

SINGLE SIGN-ON

If users have the same login ID in different LDAP servers, the single sign-on login fails. Users must enter their passwords manually instead.

KERBEROS

Even if you have configured multiple LDAP systems, you can use only one LDAP server with Kerberos authentication.

When you use multiple LDAP systems, you must enable the **Ignore realm from service ticket** property under **Kerberos > Advanced Settings**.

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.

WEBDAV

The WebDAV protocol provides a framework for users to create, change, and move documents on a server. The WebDAV protocol enables you to maintain properties related to, for example, an author or modification date.

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

ARIS ARCHITECT

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

Example

If you search for user LDAP1/user 1, the user is found.

If you search for user 1, the user is not found.

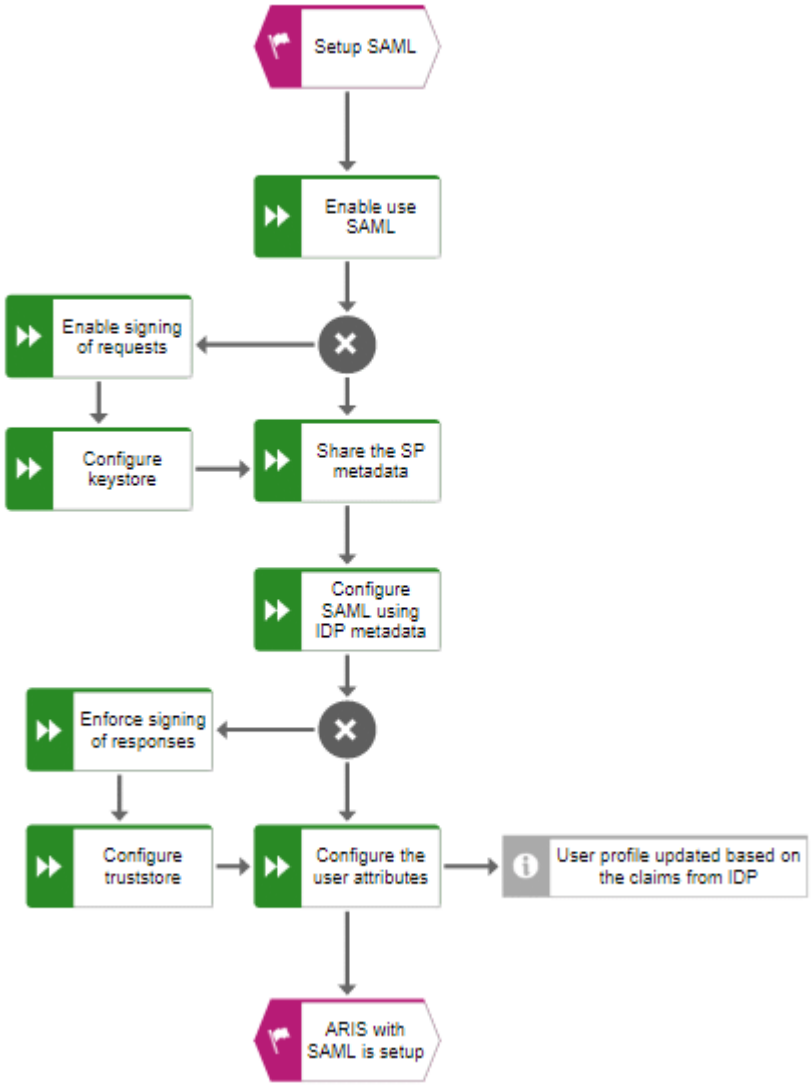
PROCESS GOVERNANCE

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

3.6 Set up SSO for LDAP with SAML

SAML (**S**ecurity **A**ssertion **M**arkup **L**anguage) 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 it enables web-based authentication scenarios including single sign-on across all ARIS runnables.

3.6.1 Overview



3.6.2 Procedure

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 metadata XML file if SAML is enabled.
- ARIS must be registered as a trusted service provider at the SAML identity provider.

Client

Your web browser supports JavaScript.

ENABLE SSO FOR THE SERVERS (SAML)

Prerequisite

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

Procedure

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User management**.
4. Click the arrow next to **SAML**.
5. Click **General**.
6. Click **Edit**.
7. Enable **Use SAML**.
8. Enter the ID of the identity provider in the **Identity provider ID** field.
9. Enter the ID of the service provider in the **Service provider ID** field, for example **UMC@<server name>**.
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.
12. Click **Save**.

OPTIONAL SAML SETTINGS

1. Click **Signature**.
2. Click **Edit**.
3. Enable the check box of the options you want to set:
   - Enforce signing of assertions
   - Enforce signing of requests
   - Enforce signing of responses
   - Enforce signing of metadata
   - Select signature algorithm
4. Click **Save**.

You have enabled the signing. If you have enabled this option, you must configure the truststore.

OPTIONAL: CONFIGURE THE KEYSTORE

1. Click **Keystore**.
2. Click **Upload**. The dialog opens. Select the keystore file on your file system and click **Upload**.
3. Click **Edit**.
4. Configure your keystore.
5. Click **Save**.

You have configured the keystore.

SHARE THE SERVICE PROVIDER (SP) METADATA

1. Click **General**.
2. Send the service provider ID to your identity provider (IDP).

CONFIGURE SAML USING IDENTITY PROVIDER (IDP) METADATA

1. Click **General**.
2. Click **Edit**.
3. Enter the identity provider ID.
4. Click **Save**.

OPTIONAL: CONFIGURE THE TRUSTSTORE

1. Click **Truststore**.
2. Click **Upload**. The dialog opens. Select the truststore file on your file system and click **Upload**.
3. Click **Edit**.
4. Configure your truststore.
5. Click **Save**.

You have configured the truststore.

CONFIGURE THE USER ATTRIBUTES

1. Click **User attributes**.
2. Click **Edit**.
3. Specify the attribute fields, for example, the first name, the last name, or the e-mail.
4. Click **Save**.

You have configured the user attributes.

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>`

   You get a metadata file. Save this file as an XML file.
3. Send the metadata file to your SAML identity provider that the metadata can be uploaded.

Your system is configured to be used with single sign-on and SAML.

TROUBLESHOOTING

You can find detailed information on SAML authentication issues in the log files of ARIS Administration located in

```
<Your installation
folder>\ARIS10.0\server\bin\work\work_umcadmin_<size>\base\logs
```

Example

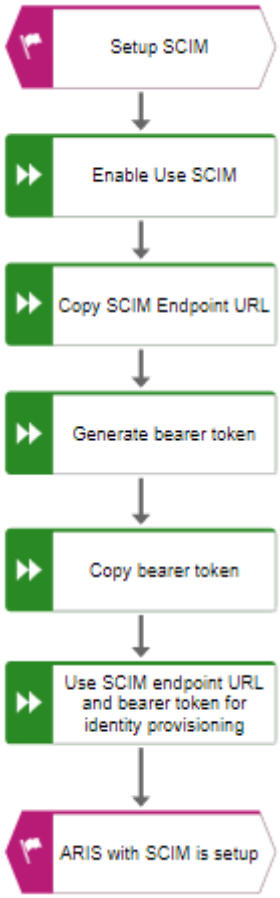
```
C:\SoftwareAG\ARIS10.0\server\bin\work\work_umcadmin_m\base\logs
```

4 Set up SCIM (ARIS Enterprise)

SCIM stands for **S**ystem for **C**ross-domain **I**dentity **M**anagement (**SCIM**) and is designed to facilitate the management of user identities in cloud-based applications and services.

ARIS supports SCIM 2.0.

4.1 Overview



4.2 Procedure

ENABLE SCIM

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

Prerequisite

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

1. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
2. Click **User Management**.
3. Click the arrow next to **SCIM**.
4. Click **General**.
5. Click **Edit**.
6. Enable **Enable Identity management service**.
7. Optional: Enable/Disable the e-mail notification for user creation. That means that if a user is created on the SCIM server side, each newly created user receives an e-mail about the creation.
8. Click **Save**.
9. Copy the end point URL and hand-over the end point URL to your identity provider for provisioning.

GENERATE BEARER TOKEN

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

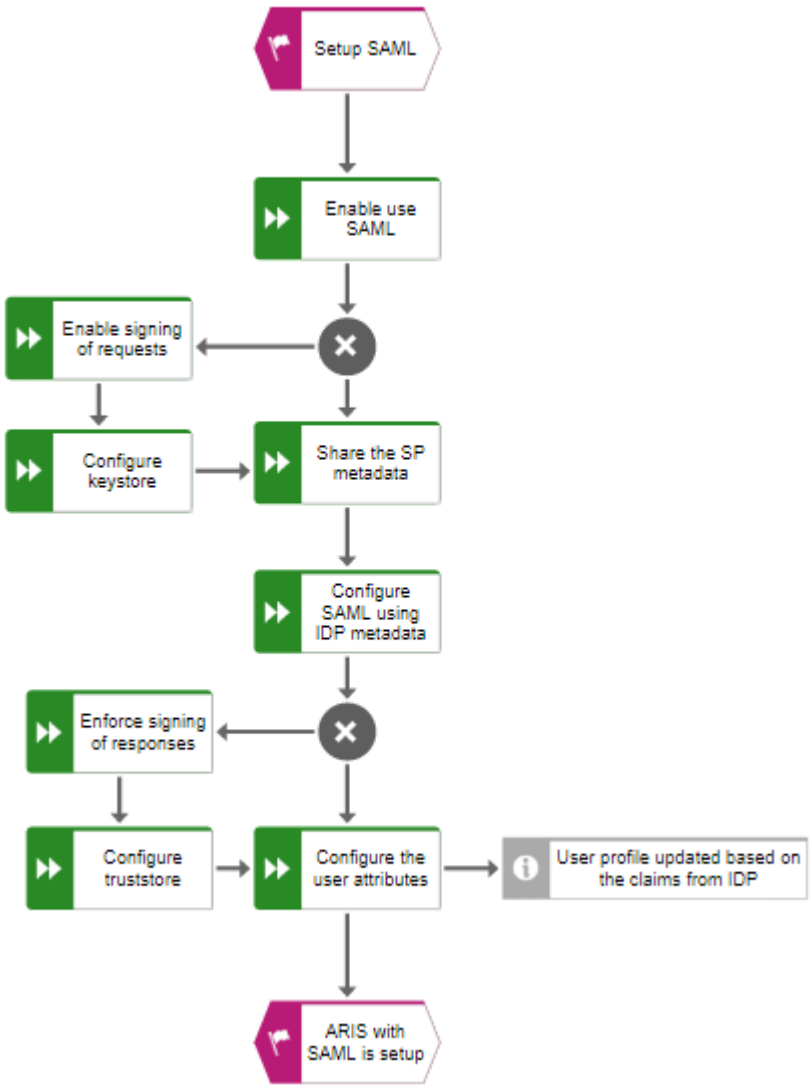
If the bearer token is newly created, the bearer token is displayed in the **SCIM bearer token** field. If a bearer token already exists, the **Generate bearer token** dialog opens and you can confirm that a new bearer token should be created. ARIS with SCIM is set up.

If you want to use single sign-on, you can use SAML 2.0 (page 18).

4.3 Set up SSO for SCIM with SAML

SAML (**S**ecurity **A**ssertion **M**arkup **L**anguage) 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 it enables web-based authentication scenarios including single sign-on across all ARIS runnables.

4.3.1 Overview



4.3.2 Procedure

Prerequisite

Server

- The SAML identity provider supports the HTTP POST binding as specified by the SAML 2.0 specification.
- SSO must be configured for the servers.
- You only have access to the metadata XML file if SAML is enabled.
- ARIS must be registered as a trusted service provider at the SAML identity provider.

Client

Your web browser supports JavaScript.

ENABLE SSO FOR THE SERVERS (SAML)

Prerequisite

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

Procedure

1. Start ARIS.
2. Click **Application launcher** > **Administration**. The **Administration** opens with the **Configuration** view.
3. Click **User management**.
4. Click the arrow next to **SAML**.
5. Click **General**.
6. Click **Edit**.
7. Enable **Use SAML**.
8. Enter the ID of the identity provider in the **Identity provider ID** field.
9. Enter the ID of the service provider in the **Service provider ID** field, for example **UMC@<server name>**.
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.
12. Click **Save**.

OPTIONAL SAML SETTINGS

1. Click **Signature**.
2. Click **Edit**.
3. Enable the check box of the options you want to set:
   - Enforce signing of assertions
   - Enforce signing of requests
   - Enforce signing of responses
   - Enforce signing of metadata
   - Select signature algorithm
4. Click **Save**.

You have enabled the signing. If you have enabled this option, you must configure the truststore.

OPTIONAL: CONFIGURE THE KEYSTORE

1. Click **Keystore**.
2. Click **Upload**. The dialog opens. Select the keystore file on your file system and click **Upload**.
3. Click **Edit**.
4. Configure your keystore.
5. Click **Save**.

You have configured the keystore.

SHARE THE SERVICE PROVIDER (SP) METADATA

1. Click **General**.
2. Send the service provider ID to your identity provider (IDP).

CONFIGURE SAML USING IDENTITY PROVIDER (IDP) METADATA

1. Click **General**.
2. Click **Edit**.
3. Enter the identity provider ID.
4. Click **Save**.

OPTIONAL: CONFIGURE THE TRUSTSTORE

1. Click **Truststore**.
2. Click **Upload**. The dialog opens. Select the truststore file on your file system and click **Upload**.
3. Click **Edit**.
4. Configure your truststore.
5. Click **Save**.

You have configured the truststore.

CONFIGURE THE USER ATTRIBUTES

1. Click **User attributes**.
2. Click **Edit**.
3. Specify the attribute fields, for example, the first name, the last name, or the e-mail.
4. Click **Save**.

You have configured the user attributes.

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>`

   You get a metadata file. Save this file as an XML file.
3. Send the metadata file to your SAML identity provider that the metadata can be uploaded.

Your system is configured to be used with single sign-on and SAML.

TROUBLESHOOTING

You can find detailed information on SAML authentication issues in the log files of ARIS Administration located in

```
<Your installation
folder>\ARIS10.0\server\bin\work\work_umcadmin_<size>\base\logs
```

Example

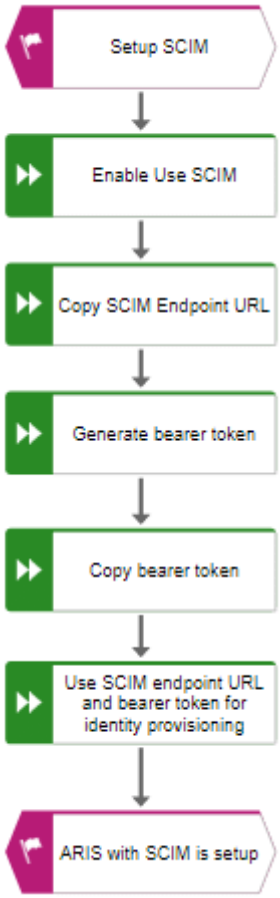
```
C:\SoftwareAG\ARIS10.0\server\bin\work\work_umcadmin_m\base\logs
```

5 Set up SCIM (ARIS Advanced Base Extension))

SCIM stands for **S**ystem for **C**ross-domain **I**dentity **M**anagement (**SCIM**) and is designed to facilitate the management of user identities in cloud-based applications and services.

ARIS supports SCIM 2.0.

5.1 Overview



5.2 Procedure

Prerequisite

You have the **ARIS Advanced Base Extension pack** license.

ENABLE THE IDENTITY MANAGEMENT SERVICE

1. Open ARIS Advanced.
2. Click **Application launcher** > **Administration**.
3. Click **Configuration management**.
4. Click **Identity management**.
5. Enable **Enable Identity management service**.
6. Optional: Enable/Disable the e-mail notification for user creation. That means that if a user is created on the SCIM server side, each newly created user receives an e-mail about the creation.
7. Click **Save**.
8. Copy the end point URL and hand-over the end point URL to your identity provider for provisioning.

GENERATE BEARER TOKEN

1. Click **Application launcher** > **Administration**.
2. Click **Configuration management**.
3. Click **Identity management**.
4. Click **Generate bearer token**. ARIS with SCIM is set up.
5. Click **Back**.

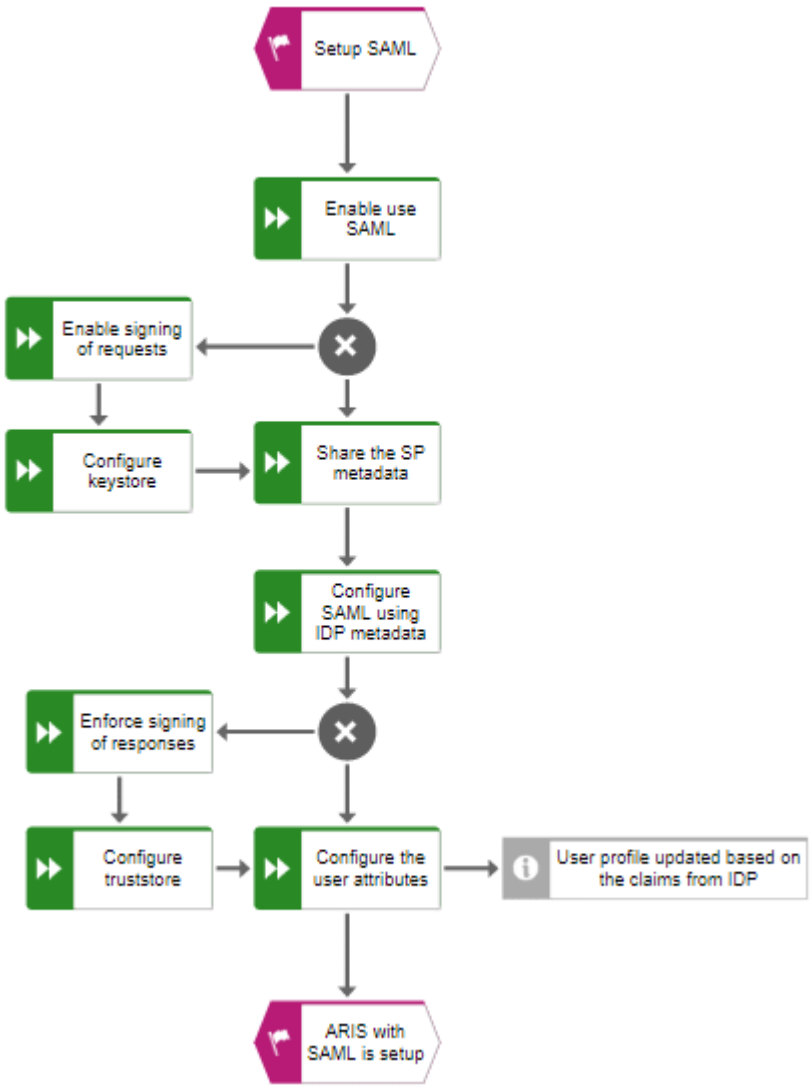
If you want to use single sign-on, you can use SAML 2.0 (page 49).

5.3 Set up SSO for SCIM with SAML

SAML (**S**ecurity **A**ssertion **M**arkup **L**anguage) 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 it enables web-based authentication scenarios including single sign-on across all ARIS runnables.

Please contact your SAML administrator before you change any configuration.

5.3.1 Overview



5.3.2 Procedure

Prerequisite

Server

- The SAML identity provider supports the HTTP POST binding as specified by the SAML 2.0 specification.
- SSO must be configured for the servers.
- You only have access to the metadata XML file if SAML is enabled.
- ARIS must be registered as a trusted service provider at the SAML identity provider.

Client

Your web browser supports JavaScript.

ENABLE SSO (SAML)

Procedure

1. Open ARIS Advanced.
2. Click **Application launcher** > **Administration**.
3. Click **Configuration management**.
4. Click **Single sign-on**.
5. Under **General**, enable **Enable single sign-on**.
6. Enter the ID of the identity provider in the **Identity provider ID** field.
7. Enter the ID of the service provider in the **Service provider ID** field, for example **UMC@<server name>**.
8. Enter the end point of the identity provider that is used for single sign-on in the **Single sign-on URL** field.
9. Enter the end point of the identity provider that is used for single log-out in in the **Single logout URL** field.
10. Click **Save**.

OPTIONAL SAML SETTINGS

1. Under **Signature**, enable the options you want to set:
   - Enforce signing of assertions
   - Enforce signing of requests
   - Enforce signing of responses
   - Enforce signing of metadata
   - Select signature algorithm
2. Click **Save**.

You have enabled the signing. If you have enabled this option, you must configure the truststore.

OPTIONAL: CONFIGURE THE KEYSTORE

1. Under **Keystore**, click **Upload**.
2. Click **Upload**. The dialog opens. Select the keystore file on your file system and click **Upload**.
3. Configure your keystore.
4. Click **Save**.

You have configured the keystore.

SHARE THE SERVICE PROVIDER (SP) METADATA

1. You can find the service provider metadata under **General**. Send the service provider ID to your identity provider (IDP).

CONFIGURE SAML USING IDENTITY PROVIDER (IDP) METADATA

1. Under **General**, enter the identity provider ID.
2. Click **Save**.

OPTIONAL: CONFIGURE THE TRUSTSTORE

1. Under **Truststore**, click **Upload**. The dialog opens. Select the truststore file on your file system and click **Upload**.
2. Configure your truststore.
3. Click **Save**.

You have configured the truststore.

CONFIGURE THE USER ATTRIBUTES

1. Under **User attributes**, specify the attribute fields, for example, the first name, the last name, or the e-mail.
2. Click **Save**.

You have configured the user attributes.

OPTIONAL: ADVANCED SETTINGS

1. Under **Advanced settings**, configure:
   - Authentication context classes
   - Authentication content comparison
   - NamedID format
   - Clock skew (in seconds)
   - Assertion lifetime (in seconds)
2. Click **Save**.

You have configured the advanced settings.

6 Legal information

6.1 Documentation scope

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

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

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

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

6.2 Support

If you have any questions on specific installations that you cannot perform yourself, contact your local Software AG sales organization (https://www.softwareag.com/corporate/company/global/offices/default.html). To get detailed information and support, use our Web sites.

If you have a valid support contract, you can contact **Global Support ARIS** at: **+800 ARISHELP**. If this number is not supported by your telephone provider, please refer to our Global Support Contact Directory.

ARIS COMMUNITY

Find information, expert articles, issue resolution, videos, and communication with other ARIS users. If you do not yet have an account, register at ARIS Community.

PRODUCT DOCUMENTATION

You can find the product documentation on our documentation Web site.

In addition, you can also access the cloud product documentation. Navigate to the desired product and then, depending on your solution, go to **Developer Center**, **User Center** or **Documentation**.

PRODUCT TRAINING

You can find helpful product training material on our Learning Portal.

TECH COMMUNITY

You can collaborate with Software AG experts on our Tech Community Web site. From here you can, for example:

- Browse through our vast knowledge base.
- Ask questions and find answers in our discussion forums.
- Get the latest Software AG news and announcements.
- Explore our communities.
- Go to our public GitHub and Docker repositories and discover additional Software AG resources.

PRODUCT SUPPORT

Support for Software AG products is provided to licensed customers via our Empower Portal (https://empower.softwareag.com/). Many services on this portal require that you have an account. If you do not yet have one, you can request it. Once you have an account, you can, for example:

- Download products, updates and fixes.
- Add product feature requests.
- Search the Knowledge Center for technical information and tips.
- Subscribe to early warnings and critical alerts.
- Open and update support incidents.