



ARIS USERS AND LICENSE MANAGEMENT

VERSION 10.0 - SERVICE RELEASE 12

April 2020

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 - 2020 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 <http://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 <http://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 <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Contents

Contents	1
1 Text conventions	1
2 Users and licenses	2
3 What is impersonation?	4
4 What license types exist?.....	5
5 When is a license consumed?	6
6 What happens when a license expires?.....	7
7 What is the difference between the license types?	8
8 What dependencies exist within the privileges?	9
9 Tenant	10
9.1 Log in to the infrastructure tenant's User Management	10
9.2 Change passwords on the infrastructure tenant	11
9.3 Log in to the ARIS Administration of a tenant	12
9.4 Change passwords on tenants	13
10 Configure single sign-on	14
10.1 Configure single sign-on using Kerberos	15
10.2 Kerberos keys	20
10.3 Configure single sign-on using SAML	23
10.4 SAML keys	26
10.5 Configure single sign-on using SCIM	34
10.6 SCIM keys	36
11 Legal information.....	38
11.1 Documentation scope	38
11.2 Data protection	39
11.3 Restrictions.....	39

1 Text conventions

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

- Menu items, key combinations, dialogs, file names, entries, etc. are displayed in **bold**.
- User-defined entries are shown as **<bold text in angle brackets>**.
- Example texts that are too long to fit on a single line, such as a long directory path, are wrapped to the next line by using ↵ at the end of the line.
- File extracts are shown in this font format:
This paragraph contains a file extract.
- Warnings have a colored background:

Warning

This paragraph contains a warning.

2 Users and licenses

For all ARIS products users are managed centrally within the user management. Using ARIS Server the user management is part of the ARIS Administration. The role specific data access is handled by license (page 5) privileges and function privileges and database specific privileges managed within the ARIS Administration and database specific privileges and filters associated to users and user groups. These database specific privileges and filters are managed within ARIS Architect for each database of a tenant.

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

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

USER MANAGEMENT WITHIN THE ARIS ADMINISTRATION

The ARIS Administration is a tool managing users, user groups, privileges, licenses, documents, and configurations for each tenant affecting all ARIS products. This ensures the single sign-on for various ARIS products. Users can also be imported from an LDAP system. ARIS Administration is available for users holding the **User administrator** and **License administrator** function privilege. Initially, only the administrative users **superuser** and **system** are available. These users are able to manage users for all tenants of your system (page 2). Users can also be managed using the command line tools of ARIS Administration.

If you have installed an ARIS Risk & Compliance Manager version, using its own ARIS Administration or you are using ARIS Publisher Server, you can force these components to use the ARIS Administration of the ARIS Server in order to manage users centrally. Therefore you must reconfigure ARIS Risk & Compliance Manager and/or force ARIS Publisher Server to use the specific ARIS Administration.

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

1. Change the passwords of the **superuser** user and the **system** user. (page 13)
2. Make sure to assign all required license privileges to the **system** user, such as ARIS Architect. Otherwise the **system** user cannot perform administrative actions, such as running scheduled reports. For detailed information on license and user management and security settings refer to the **Manage ARIS Connect** online help chapter.
3. Import the license if it has not been imported during the setup process.
4. Create users or import them from the LDAP system.
5. Create user groups or import them from the LDAP system.

6. Assign users to user groups.
7. Assign privileges.

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

All users and user groups managed in the ARIS Administration are available in every existing or future databases of the tenant. In each database product specific privileges must be assigned in ARIS Architect. To do so, proceed as described in the chapter **Managing Users** of the ARIS Architect Online Help.

USER MANAGEMENT WITHIN ARIS ARCHITECT

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

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

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

1. Create databases.
2. Assign database specific function privileges.
3. Assign database specific access privileges.
4. Assign database specific filters.
5. Provide the URL **http://<IP address or fully-qualified host name>:<load balancer port>/#<tenant name>/home**, for example, **http://aris.connect.sag/#default/home** to all users using ARIS Connect.

All authorized users have access to licensed ARIS products.

Privileges and filters must be assigned for each additional database.

Further information is available in the ARIS Administration online help.

3 What is impersonation?

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

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

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

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

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

4 What license types exist?

You can use only one license type for each product. Exceptions are the **Named user** and **Cross-client** license types.

LICENSE TYPES FOR CLIENT PRODUCTS

The license types for client products must be assigned manually to users or user groups. You can increase the number of licenses by installing additional licenses.

NAMED USER

Users assigned to this license type have guaranteed login as the license is registered in their name. The number of licenses that can be assigned is specified in the license file.

CONCURRENT USER

For this license type, the number of users who can log in at the same time is specified. The assigned users share the available licenses. If the number of users logged in is the same as the number of available licenses, no other users can log in. The user must wait until another user logs off. However, the administrator can end the sessions of users.

CROSS-CLIENT

This license type corresponds to a license of the **Named user** type. However, it can be imported and used for various tenants. It is intended for administrators who manage several tenants. The assigned users can log in with all tenants.

SERVER LICENSES

The license types for server products are activated automatically after the import.


5 When is a license consumed?

A license is consumed as soon as a user logs in and a session is created. Please note that a license is not only consumed when a user starts working, like creating models in ARIS Connect or administrating processes. If various licenses are assigned to a user, the license with the higher value is consumed first.

Example

User A is assigned to the licenses **ARIS Connect Viewer** and **ARIS Connect Designer** (both **Concurrent user** license type). After login, the **ARIS Connect Designer** license is consumed.

6 What happens when a license expires?

Expired licenses are marked in the license overview: . Users or groups can no longer be assigned. Login is impossible with an expired license.

Before deleting licenses, back up user data, if required, in order to be able to reuse them when new license are available. In the configuration, you can specify that administrators are notified before a license expires.

7 What is the difference between the license types?

	Concurrent user	Named user
Assignment	Via user or user group	Via user or user group
License volume	Unlimited	Limited number
Guaranteed login	No	Yes
Term of guaranteed login	Current session	Unlimited

8 What dependencies exist within the privileges?

- There are certain license privileges that you cannot assign to a user in combination with others. For example, you cannot assign ARIS Architect and ARIS Designer to a user at the same time.
- You can only activate the subgroups of a license privilege if the superior license privilege is activated. If you remove a superior license privilege of a user, the user also automatically loses the assignment to the subgroups.

9 Tenant

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

9.1 Log in to the infrastructure tenant's User Management

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

You only need to log in to the User Management

- to change the **superuser**'s and the **system** user's passwords to prevent unauthorized access
- to configure the Tenant Management tool

After the installation only the administrative users **superuser** or **system** can login. Manage users, user groups, privileges, licenses, documents, configurations, and processes for all ARIS products. For detailed information please refer to the ARIS Administration's online help.



Procedure

1. Click the link **<http://localhost/umc>** or **<IP address or fully-qualified host name>/umc**. The login dialog of the ARIS Administration opens.
2. Enter the user name **superuser** and the password **superuser**.
3. Change the tenant name if **default** is not the one you want to login to.
4. Click **Log in**.

The ARIS Administration opens.

9.2 Change passwords on the infrastructure tenant

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

1. Log in to the infrastructure tenant's User Management (page 10).
2. Click  **User management**, and select **Users**. The list of users is displayed.
3. Enter **superuser** into the search box. The search result is shown.
4. Click **superuser**. The user data (details) is displayed.
5. Click  **Edit**.
6. Enable the **Change password** check box. The **Password** and **Confirm password** boxes are displayed.
7. Enter a new password, and reenter it. If you want to use the webMethods integration, passwords may not contain a colon.
8. Click **Save**.
9. Change the **system** user's password too.

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

9.3 Log in to the ARIS Administration of a tenant

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



Procedure

1. Open your browser and enter **http://<IP address or fully-qualified host name>:<port number other than default>/#<tenant name>/adminSettings**. You must enter the port number only if you have changed or redirected the standard port **80**. The login dialog opens.
2. Enter the user name **superuser** and the password **superuser**. This user only has access to the ARIS Administration of the server.
3. Click **OK**. ARIS Administration opens.
4. Click the required tab.

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

9.4 Change passwords on tenants

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

1. Log in to the tenant's ARIS Administration (page 12).
2. Click  **User management**, and select **Users**. The list of users is displayed.
3. Enter **superuser** into the search box. The search result is shown.
4. Click **superuser**. The user data (details) is displayed.
5. Click  **Edit**.
6. Enable the **Change password** check box. The **Password** and **Confirm password** boxes are displayed.
7. Enter a new password, and reenter it. If you want to use the webMethods integration, passwords may not contain a colon.
8. Click **Save**.
9. Change the **system** user's password too.

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

10 Configure single sign-on

You can configure single sign-on (SSO) using Kerberos (page 15) or SAML (page 23). When using Kerberos, this provides access to all ARIS runnables as soon as a user has logged in to the domain. When using SAML, this provides access to all ARIS Connect runnables as soon as a user has logged in to the domain.

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

10.1 Configure single sign-on using Kerberos

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

Kerberos is a network authentication, allowing nodes to communicate using an invisible network and to securely make their identity known to each other. Kerberos is the recommended method for user authentication in Microsoft® Windows networks. In addition, it is widely used with Linux operating systems and is designed for use with all major platforms. It is designed to provide a strong authentication for client/server applications, like web applications where the browser is the client. It is also the recommended way to authenticate users in a MS Windows network and it replaces the outdated and relatively insecure NT LAN Manager (NTLM).

Please contact your LDAP administrator before you change any configuration.

Prerequisite

Server

- Users who want to use SSO must have a valid Microsoft® Active Directory Domain Services user login.
- This user is available in ARIS Administration.
- ARIS Administration authenticates against LDAP.
- Microsoft® Active Directory Domain Services supports Kerberos-based authentication (default) and the service principal name of the ARIS Server is entered in the following format: **HTTP/<hostname>**, for example, **HTTP/mypc01.my.domain.com**.

Client

- The client computers and servers are connected to the same Microsoft® Active Directory Domain Services.
- The browser has been configured accordingly.

The following steps must be taken to use SSO:

Procedure

1. A technical user must be created in the Microsoft® Active Directory Domain Services.
2. A service principal name must be registered on the technical user.
3. The single sign-on configuration options must be set in ARIS Administration.
4. The client application must be configured to use single sign-on.

You configured SSO on client side.

CREATING A TECHNICAL USER

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

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

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

ktab -a <TECHUSER_USER_PRINCIPAL_NAME> -n 0 -append -k umc.keytab - for example **ktab -a aristechuser@MYDOMAIN.COM -n0 -append -k umc.keytab**.



CONFIGURATION OPTIONS IN ARIS ADMINISTRATION

You need to configure SSO for the servers.

Prerequisite

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



Procedure

1. Start ARIS Connect.
2. Click your name or the  **User menu** icon.
3. Click **Administration**.
4. Click  **Configuration**.
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_etypes = 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_etypes = 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_etypes = 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. You find this file on your installation medium under **Add-ons\Kerberos**.
8. Click  **Edit**.
9. Enable **Use Kerberos**.
10. In the **Principal** field, enter the technical user name given by the administrator.
If the Service Principal Name in the keytab is, for example, **mypc01@MY.DOMAIN.COM**, the values of the property **com.company.aris.umc.kerberos.servicePrincipalName** must contain the Service Principal Name exactly as specified in the keytab file.
11. In the **Realm** field, configure the realm for the Kerberos service. Enter the fully qualified domain name in uppercase letters.
Example: **MYDOMAIN.COM**.
12. In the **KDC** field, configure the fully qualified name of the KDC to be used.
13. **Optional:**
 - a. Click **Advanced settings**.
 - b. Enable **Debug output**.

The debug output of the program that the user wishes to log into is saved in the file **system.out** of the respective program. For user management, for example, this is located in the directory **<ARIS installation directory>/work_umcadmin_m/base/logs**.

You have configured SSO using Kerberos in ARIS Administration.

CLIENT CONFIGURATION

Configure the browser settings to allow SSO. SSO has been tested with the following browsers:

- Microsoft® Internet Explorer® (version 11 or higher)
- Mozilla Firefox®

Prerequisite

- You have the **Technical configuration administrator** function privilege.
- SSO must be configured for the servers.
- The browser used supports a Kerberos-based authentication.

You need to empty the Kerberos ticket cache of each client first, in order to avoid obsolete tickets if Microsoft® Active Directory Domain Services were changed. Delete the Kerberos ticket cache by executing the command **klist.exe purge**. If the purge program is not available on the client computer, you can also simply log off the client computer from the domain and log in again.

MICROSOFT® INTERNET EXPLORER®

Microsoft® Internet Explorer® supports Kerberos authentication only if the ARIS Server is part of your local intranet.

Procedure

1. Start Microsoft® Internet Explorer®.
2. Click **Tools > Internet Options**.
3. Activate the **Security** tab and click **Local Intranet**.
4. Click **Sites**, and select **Advanced**.
5. Add the URL of the ARIS Server that was configured for SSO. Add the DNS host name and the IP address of the ARIS Server.
6. Optional: Disable the **Require server verification (https:) for all sites in this zone** check box.
7. Click **Close**, and select **OK**.
8. Click **Custom level** and make sure that no user-defined settings affect your new settings.
9. Find the **User Authentication** section. Verify whether the **Automatic logon only in Intranet zone** option is enabled.
10. Click **OK**.
11. Close and restart Microsoft® Internet Explorer®.

MOZILLA FIREFOX®

In Mozilla Firefox®, you can define trustworthy sites using the computer name, IP address, or a combination of both. You can use wildcards.

Procedure

1. Start Mozilla Firefox®.
2. Enter **about:config** in the address box and press **Enter**. Confirm a message, if required.
3. Enter **network.negotiate** in the **Search** box and press **Enter**, if required.
4. Double-click **network.negotiate-auth.trusted-uris**.
5. Enter the computer name or the IP address of the ARIS Server that you configured for SSO, and click **OK**.
6. Close and restart Mozilla Firefox®.

If you prefer to use an encryption stronger than AES 128bit and this is allowed in your country, replace the JCE Policy file of the JDK of your ARIS Server with the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 (<http://www.oracle.com/technetwork/java/javase/downloads/index.html>). This allows unlimited key length.

If you cannot replace the Policy files, but still want to use SSO, you need to apply a procedure allowed by the JDK for encrypting Kerberos tickets, for example, AES 128bit.

10.2 Kerberos keys

You can configure Kerberos as required.

Properties that are highlighted as cross-tenant properties can only be changed using ARIS Cloud Controller Command-line Tool. To change the settings, enter the following:

```
reconfigure umcadmin_<size of your installation, s, m, or l> JAVA-D<property name>=<value>
```

Example

```
reconfigure umcadmin_m JAVA-Dcom.aris.umc.loadbalancer.url="https://myserver.com"
```

GENERAL

Key	Description	Valid input	Example
com.aris.umc.kerberos.active	Use Kerberos Specifies whether a Kerberos-based login is allowed.	True, False	
com.aris.umc.kerberos.kdc	KDC Specifies the fully qualified name of the central Key Distribution Center (KDC) . This is usually the fully qualified host name of the LDAP server.	String	mykdc.mydomain.com
com.aris.umc.kerberos.realm	Realm Specifies the realm of Kerberos tickets. Fully qualified domain name in uppercase letters.	String	MY.CORP.SOFTWAREA G.COM

Key	Description	Valid input	Example
com.aris.umc.kerberos.servicePrincipalName	<p>Principal</p> <p>Specifies the name of the technical user used for verifying Kerberos tickets.</p> <p>If Kerberos is used, each user, computer or service provided by a server must be defined as a principal.</p>	String	MyLogin
com.aris.umc.kerberos.keyTab	<p>Key table</p> <p>Specifies the location of the keytab file that is used for Kerberos tickets.</p> <p>The file can be uploaded directly.</p>	String	C:/safePlace/krb-umc.keytab
com.aris.umc.kerberos.config	<p>Configuration file</p> <p>Storage location of the configuration file for Kerberos.</p> <p>The file can be uploaded directly.</p>	String	./config/Kerberos/krb5.conf

ADVANCED SETTINGS

Key	Description	Valid input	Example
com.aris.umc.kerberos.debug	<p>Debug output</p> <p>Specifies whether debug output is allowed for Kerberos operations.</p>	True, False	
com.aris.umc.kerberos.allowLocalUsers	<p>Allow local users</p> <p>Specifies whether the LDAP connection is mandatory for Kerberos-based login. If this option is enabled, Kerberos is used for the login of local users also.</p>	True, False	

Key	Description	Valid input	Example
com.aris.umc.kerberos.validateuser	Ignore realm from service ticket Specifies whether or not the realm defined for the user principal name provided in the Kerberos ticket is to be ignored. The default value is false .	True, False	
com.aris.umc.kerberos.tenant	Default tenant Specifies the default tenant for a Kerberos-based login. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual .	True, False	

10.3 Configure single sign-on using SAML

Single sign-on with SAML can be used with applications running in a browser.

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

Please contact your LDAP administrator before you change any configuration.

Prerequisite

Server

- Users who want to use SSO must have a valid Microsoft® Active Directory Domain Services user login.
- This user is available in ARIS Administration.
- ARIS Administration authenticates against LDAP.
- The SAML identity provider supports the HTTP POST binding as specified by the SAML 2.0 specification.

Client

Web browser supports JavaScript.

The following steps must be taken to use SSO:

Procedure

1. The single sign-on configuration options must be set in the ARIS Administration.
2. ARIS must be registered as a trusted service provider at the SAML identity provider.

You configured SSO.




CONFIGURATION OPTIONS IN ARIS ADMINISTRATION

You need to configure SSO for the servers.

Prerequisite

- You have the **Technical configuration administrator** function privilege.
- If you use multiple LDAP systems, the user names must be unambiguous through all LDAP systems. Otherwise no SSO is possible.

Procedure

1. Start ARIS Connect.
2. Click your name or the  **User menu** icon.
3. Click **Administration**.
4. Click  **Configuration**.
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 configured SSO using SAML in ARIS Administration. If you use multiple LDAP systems, the user names must be unambiguous through all LDAP systems. Otherwise no SSO is possible.

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

REGISTER ARIS AS A TRUSTED SERVICE PROVIDER

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

Procedure

1. Open a browser.
2. Enter the following URL into the address bar:
`https://<SERVERNAME>/umc/rest/saml/metadata.xml?tenant=<TENANTID>`
You get a meta data file. Save this file as XML file.
3. Upload the meta data file into your SAML identity provider.

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

TROUBLESHOOTING

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

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

Example

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

10.4 SAML keys

You can configure SAML as required.

Properties that are highlighted as cross-tenant properties can only be changed using ARIS Cloud Controller Command-line Tool. To change the settings, enter the following:

```
reconfigure umcadmin_<size of your installation, s, m, or l> JAVA-D<property name>=<value>
```

Example

```
reconfigure umcadmin_m JAVA-Dcom.aris.umc.loadbalancer.url="https://myserver.com"
```

GENERAL

Key	Description	Valid input	Example
com.aris.umc.saml.active	Use SAML Specifies whether an SAML-based login is allowed.	true, false	false
com.aris.umc.saml.binding	Binding Specifies the binding used for sending authentication requests to the identity provider. Defines how the redirecting of the authentication is performed. The options are Redirect or POST .		POST
com.aris.umc.saml.identity.provider.id	Identity provider ID Specifies the ID of the identity provider.	String	
com.aris.umc.saml.service.provider.id	Service provider ID Specifies the ID of the service provider.	String	

Key	Description	Valid input	Example
com.aris.umc.saml.identity.provider.sso.url	<p>Single sign-on URL</p> <p>Specifies the end point of the identity provider that is used for single sign-on.</p>		
com.aris.umc.saml.identity.provider.logout.url	<p>Single logout URL</p> <p>Specifies the end point of the identity provider that is used for single log-out.</p>		

SIGNATURE

Key	Description	Valid input	Example
com.aris.umc.saml.signature.assertion.active	<p>Enforce signing of assertions</p> <p>Enforces that SAML assertions must be signed. If set, all assertions received by the application must be signed. Assertions sent by the application are signed.</p>	true, false	false
com.aris.umc.saml.signature.request.active	<p>Enforce signing of requests</p> <p>Enforces that the SAML authentication requests must be signed. If set, all requests received by the application must be signed. Requests sent by the application are signed.</p>	true, false	false
com.aris.umc.saml.signature.response.active	<p>Enforce signing of responses</p> <p>Enforces that the SAML response must be signed. If set, all responses received by the application must be signed. Responses sent by the application are signed.</p>	true, false	false

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

KEYSTORE

Key	Description	Valid input	Example
com.aris.umc.saml.keystore.location	Keystore Specifies the location of the keystore file used for validating SAML assertions. The keystore must have been uploaded previously.		
com.aris.umc.saml.keystore.alias	Alias Specifies the alias name that is used to access the keystore.	String	
com.aris.umc.saml.keystore.password	Password Specifies the password that is used to access the keystore.	String	

Key	Description	Valid input	Example
com.aris.umc.saml.keystore.type	<p>Type</p> <p>Specifies the type of the keystore to be used. The keystore type can be selected from a list.</p>	String	JKB

TRUSTSTORE

Key	Description	Valid input	Example
com.aris.umc.saml.truststore.location	<p>Truststore</p> <p>Specifies the location of the truststore file used for validating SAML assertions. The truststore must have been uploaded previously.</p>		
com.aris.umc.saml.truststore.alias	<p>Alias</p> <p>Specifies the alias to be used for accessing the truststore.</p>	String	
com.aris.umc.saml.truststore.password	<p>Password</p> <p>Specifies the password to be used for accessing the truststore.</p>	String	
com.aris.umc.saml.truststore.type	<p>Type</p> <p>Specifies the type of the truststore.</p>	String	JKB

USER ATTRIBUTES

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

ADVANCED SETTINGS

Key	Description	Valid input	Example
com.aris.umc.saml.login.mode.dn.active	Login using DN Specifies whether login is to be tried using the fully qualified name instead of the user name.	true, false	
com.aris.umc.saml.login.mode.keyword.active	Decompose DN Specifies whether the fully qualified name is to be decomposed.	true, false	
com.aris.umc.saml.login.mode.keyword.name	Keyword Specifies which part of the fully qualified name is to be used for login.	true, false	
com.aris.umc.saml.auth.context.classes.refs	Authentication context classes Specifies the authentication context classes to request, meaning which strength of the authentication is defined. For example, you specify that users must use Kerberos if you define Microsoft® Windows as the Authentication context class and the Authentication context comparison as exact .	String	
com.aris.umc.saml.auth.context.comparison	Authentication context comparison Specifies the authentication context comparison to request, meaning you specify whether other authentication procedures are allowed or not. For example, you specify that users must use Kerberos if you define Microsoft® Windows as the Authentication context class and the Authentication context comparison as exact .	String	

Key	Description	Valid input	Example
com.aris.umc.saml.auth.nameid.format	<p>NameID format</p> <p>Specifies in which format the user ID is transferred to ARIS Administration.</p>	String	
com.aris.umc.saml.login.users.create	<p>Automatically create user</p> <p>Defines whether or not the user specified in the SAML assertion should be created automatically if the user does not already exist. The default value is false. The following restrictions apply to automatically created users:</p> <ul style="list-style-type: none"> ▪ The Login attribute is set to the name specified in the assertion. ▪ The distinguished name attribute is set to the name specified in the assertion (only if the name is in an appropriate format). ▪ A manual login is not possible if the password and e-mail attributes are not maintained. 	true, false	false
com.aris.umc.saml.assertion.timeoffset	<p>Clock skew (in seconds)</p> <p>Specifies the time offset between identity provider and service provider in seconds. Assertions are accepted if they are received within the permitted time frame.</p>		60
com.aris.umc.saml.service.provider.urls	<p>Allowed service provider URLs</p> <p>Comma-separated list of service provider URLs that are allowed to request that the user administration initiates the use of SSO.</p>		
com.aris.umc.saml.assertion.ttl	<p>Assertion lifetime (in seconds)</p> <p>Specifies the maximum lifetime of a SAML assertion in seconds.</p>		10

Key	Description	Valid input	Example
com.aris.umc.saml.service.provider.assertion.consumer.url.override	Assertion consumer service URL Specifies that the Assertion Consumer Service URL used in SAML authentication requests can be overwritten. The URL must be specified in the format of http(s)://hostname/umc/rest/saml/itsso . If no specification is made, the URL is derived from the HTTP request.		
com.aris.umc.saml.tenant	Default tenant Specifies the default tenant that is to be used for the SAML-based login. Cross-tenant property that can only be changed using ARIS Cloud Controller. For more information, refer to ARIS Cloud Controller (ACC) Command-line Tool manual .	String	default

10.5 Configure single sign-on using SCIM

You can use single sign-on using SCIM. Separate login to ARIS components is not required. The **System for Cross-Domain Identity Management** is designed to facilitate the management of user identities in cloud-based applications and services.

ARIS supports SCIM 2.0.

Please contact your SCIM administrator before you change any configuration (page 36).

Prerequisite

Server

- Use SCIM to onboard the users to ARIS Administration.
- Use SSO for authentication.

The following steps must be taken to use SSO:

Procedure

1. The single sign-on configuration options must be set in the ARIS Administration.
2. ARIS must be registered as a trusted service provider at the SAML identity provider.

You configured SSO.




CONFIGURATION IN ARIS ADMINISTRATION

You need to configure SSO for the servers.

Prerequisite

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

Procedure

1. Start ARIS Connect.
2. Click your name or the  **User menu** icon.
3. Click **Administration**.
4. Click  **Configuration**.
5. Click **User management**.
6. Click the arrow next to **SCIM**.
7. Click **General**.
8. Click  **Edit**.
9. Enable **Use SCIM**.

TROUBLESHOOTING

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

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

Example

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

10.6 SCIM keys

You can configure SCIM as required.

GENERAL

Key	Description	Valid input	Example
com.aris.umc.scim.active	<p>Use SCIM</p> <p>Enables SCIM support for User Management.</p>	True, False	False
com.aris.umc.scim.endpoint.url	<p>SCIM end point URL</p> <p>Specifies the end point URL used for SCIM. You cannot change this property.</p>	<loadbalance rurl>/umc/sci m/v2/{tenant }	
com.aris.umc.scim.basic.auth.active	<p>Basic authentication</p> <p>Enables the authentication scheme using the HTTP basic standard. The default value is true.</p>	True, False	True
com.aris.umc.scim.bearer.token.active	<p>Bearer token</p> <p>Enables the authentication scheme using the bearer token standard. The default value is true.</p>	True, False	True
com.aris.umc.scim.token.expiry.day	<p>Token lifetime (in days)</p> <p>Specifies that the bearer token will expire after this period of time in days.</p>	Integer	365

ADVANCED SETTINGS

Key	Description	Valid input	Example
com.aris.umc.scim.service.provider.advance.settings.patch.support	<p>Patch support</p> <p>The patch support is an optional server functionality that enables clients to update one or more attributes of a SCIM resource, for example a user or a user group, using a sequence of operations to add, remove, or replace values. The default value is true.</p>	True, False	True
com.aris.umc.scim.service.provider.advance.settings.change.password.support	<p>Change password support</p> <p>Enables the support for changing a user password. This means that if a user changes the password in the SCIM system, the password is also changed for ARIS. The default value is false.</p>	True, False	False
com.aris.umc.scim.service.provider.filter.support	<p>Filter support</p> <p>Specifies that clients can discover the filter capabilities of the service provider. Clients use the Filter attribute of the service provider's configuration end point. If filtering is enabled, not all users or user groups are transferred to ARIS, but only a subset. The default value is true.</p>	True, False	True
com.aris.umc.scim.user.profile.photo.support	<p>Profile picture support</p> <p>Specifies whether a profile picture is supported. The default value is false.</p>	True, False	False

11 Legal information

11.1 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.

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 Client	Refers to all programs that access shared databases by using ARIS Server.
ARIS Download Client	Refers to an ARIS Client that can be accessed using a browser.

11.2 Data protection

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

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

11.3 Restrictions

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 your product contains ARIS document storage, the following applies:

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

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

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

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

Some restrictions may apply regarding the use of process administration, ARIS Administration, ARIS document storage, and ARIS Process Board, and the generation of 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.