ARIS

USERS AND LICENSE MANAGEMENT

Version 10.0 - Service Release 1

July 2017

Contents

1 Legal notices 1

2 Text conventions 2

3 Users and licenses 3

4 What is impersonation? 5

5 Tenant 6

5.1 Log into the infrastructure tenant's User Management 6
5.2 Change passwords on the infrastructure tenant 7
5.3 Log into the tenant's ARIS Administration 8
5.4 Change passwords on tenants 9

6 Configure single sign-on 10

6.1 Configure Single Sign-On using Kerberos 10
6.2 Kerberos keys 17
6.3 Configure Single Sign-On using SAML 19
6.4 SAML keys 22

1 Legal notices

This manual describes the settings and features as they were at the time of print. Since manual and software are subject to different production cycles, the description of settings and features may differ from actual settings and features. Information about discrepancies is provided in the Readme file that accompanies the product. Please read this file and take the information into account when installing, setting up, and using the product.

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

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

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

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

Name	Includes
ARIS products	Refers to all products to which the license regulations of Software AG standard software apply.
ARIS Clients	Refers to all programs, e.g., ARIS Architect or ARIS Designer that access shared databases via ARIS Server.
ARIS Download clients	Refers to ARIS clients that can be started from a browser.

2 Text conventions

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

- Menu items, key combinations, dialogs, file names, entries, etc. are displayed in **bold**.
- User-defined entries are shown **<in bold and in angle brackets>**.
- Single-line example texts (e.g., a long directory path that covers several lines due to a lack of space) are separated by ↵ at the end of the line.
- File extracts are shown in this font format:

  ```
  This paragraph contains a file extract.
  ```
- Warnings have a colored background:

  Warning

  This paragraph contains a warning.

3 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 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 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 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 3). Users can also be managed using the ARIS Administration's command line tools.

If you are going to manage users within the ARIS Administration make sure to have the ARIS Risk & Compliance Manager reconfigured and that you have forced 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 9)
2. Import the license if it has not been imported during the setup process.
3. Create users or import them from the LDAP system.
4. Create user groups or import them from the LDAP system.
5. Assign users to user groups.
6. 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, please also to the ARIS Architect online help chapter **Manage users**.

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 privileges and filters.
3. Provide the URL **http://<IP address or fully-qualified host name>:<load balancer port>/#<tenant name>/home**, e.g. **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's online help.

4 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, e.g., 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, e.g., **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 user **superuser** requires the following function privileges in all operational tenants:

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

5 Tenant

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

5.1 Log into the infrastructure tenant's User Management

After the installation of ARIS Server, two tenants are available. The operation 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 into 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.

5.2 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 into the infrastructure tenant's User Management (page 6).
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.

5.3 Log into the tenant's ARIS Administration

The ARIS Administration is a tool to manage users, user groups, privileges, licenses, documents, and configurations for each tenant of all ARIS products. This ensures the 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 server's ARIS Administration.
3. The ARIS Administration's **Configuration > User management** tab opens.
4. Click the required tab.

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

5.4 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 into the tenant's ARIS Administration (page 8).
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.

6 Configure single sign-on

You can configure single sign-on (SSO) using Kerberos (page 10) or SAML (page 19).

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.

6.1 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 protocol that allows computers to communicate over a none-secure network to prove their identity interrelated in a secure manner by using a symmetric key cryptography during certain phases of authentication. Kerberos is the de facto standard authentication protocol used in MS Active Directory environments. 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). Besides this, it is widely used in Linux environments and there exist implementations for every major platform.

Please contact your LDAP administrator before you change any configuration.

Prerequisite

Server

- Users who want to work with SSO have a valid user account in the Microsoft Active Directory Domain Services.
- The users exist in the ARIS Administration.
- Microsoft Active Directory Domain Services supports a Kerberos-based authentication (default) and the service principal name of the ARIS Server is entered in the following format: **HTTP/<hostname>**, e.g. **HTTP/mypc01.my.domain.com**.

Client

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

The following steps must be taken to use SSO:

Procedure

1. A technical user must be created in the MS Active Directory.
2. A service principal name must be registered on the technical user.
3. The Single Sign-On configuration options must be set in the 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. This user must be created in the Microsoft Active Directory 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 without being prompted for a password. The most common use of keytab files is to allow scripts to authenticate against the Microsoft Active Directory 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 - e.g. **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. Log in to the ARIS Administration.
2. Click the arrow next to your name.
3. Click **Administration**.
4. Click **Configuration**.
5. Switch to **User management**.
6. Select **Kerberos/SPNEGO**.
7. To activate SSO, find the string

   com.aris.umc.kerberos.active

   Set this configuration key to **true**.
8. Select

   com.aris.umc.kerberos.config

   and upload the Kerberos configuration by clicking into the field.

   In case the Kerberos configuration file is not available, create a new one. Name it e.g. **krb5.conf**, add the following lines and adapt the configuration to your requirements.

   ```
   [libdefaults]
   default_tgs_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1 aes128-cts
   aes128-cts-hmac-sha1-96 aes256-cts aes256-cts-hmac-sha1-96 rc4-hmac
   arcfour-hmac arcfour-hmac-md5
   default_tkt_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1 aes128-cts
   aes128-cts-hmac-sha1-96 aes256-cts aes256-cts-hmac-sha1-96 rc4-hmac
   arcfour-hmac arcfour-hmac-md5
   permitted_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1 aes128-cts
   aes128-cts-hmac-sha1-96 aes256-cts aes256-cts-hmac-sha1-96 rc4-hmac
   arcfour-hmac arcfour-hmac-md5
   ```
9. Upload this file.
10. In the ARIS Administration, upload the generated Kerberos key tab file by clicking into the field

    com.aris.umc.kerberos.keyTab
11. In the ARIS Administration, find the following string and configure the username of the technical user.

    com.aris.umc.kerberos.servicePrincipalName

    If the service principal name in the keytab is e.g. **mypc01@MY.DOMAIN.COM** then the values of the properties **com.aris.umc.kerberos.servicePrincipalName** must contain the service principal name specified in the keytab.
12. In the ARIS Administration, find the following string and configure the realm for the Kerberos service. Enter the fully qualified name of the domain in uppercase.

    com.aris.umc.kerberos.realm

The values of the properties **com.aris.umc.kerberos.realm** must contain the fully qualified domain name - e.g. **MYDOMAIN.COM**.

13. In the ARIS Administration, find the following string and configure the fully qualified name of the KDC to be used:

    com.aris.umc.kerberos.kdc

14. **Optional:** In the ARIS Administration, find the following string and define the list of IP addresses for which you want to enable SSO (**whitelist**):

    com.aris.umc.kerberos.whitelist

    Each entry in the list must begin in an individual line:

    Example

    ```
    192.168.100.1
    192.168.100.*
    10.0.0.*
    #Allow all IPs
    *.*.*.*
    ```

15. **Optional:** In the ARIS Administration, find the following string and configure the debug mode for Kerberos operations:

    com.aris.umc.kerberos.debug=true

Example

The following can be configures in the ARIS Administration.

```
com.aris.umc.kerberos.active=true
com.aris.umc.kerberos.config=/etc/krb5.conf
com.aris.umc.kerberos.keyTab=C:/safePlace/krb-umc.keytab
com.aris.umc.kerberos.whitelist=./config/Kerberos/krb-ip-whitelist.conf
com.aris.umc.kerberos.servicePrincipalName=mypc01
com.aris.umc.kerberos.realm=MY.DOMAIN.COM
com.aris.umc.kerberos.kdc=mykdc01.my.domain.com
com.aris.umc.kerberos.whitelist=./config/Kerberos/krb-ip-whitelist.conf
com.aris.umc.kerberos.debug=false
```

CLIENT CONFIGURATION

Configure the browser settings to allow SSO. Please refer to the hardware and software requirements (see ARIS System Requirements on DVD or Empower (http://documentation.softwareag.com/aris/aris9.htm)).

MICROSOFT INTERNET EXPLORER

Microsoft Internet Explorer supports Kerberos authentication only if the ARIS Server is a component of your local Intranet.

Procedure

1. Launch Microsoft Internet Explorer.
2. Select **Tools > Internet Options**.
3. Activate the **Security** tab and click **Local Intranet**.
4. Click the **Sites** button and then the **Advanced** button.
5. Add the URL for the ARIS Server that has been configured for SSO. Add both the DNS host name and the IP address for ARIS Server.
6. Optional: If users need to access the ARIS Server without https, disable **Require server verification (https:) for all sites in this zone**.
7. Click **Close** and then **OK**.
8. Click the **Custom level** button and make sure that no user-defined settings impede your new settings.
9. Scroll to the **User Authentication** section. Check whether **Automatic logon only in Intranet zone** is activated.
10. Click **OK** to close the dialogs.
11. Close and restart Microsoft Internet Explorer.

MOZILLA FIREFOX

In Mozilla Firefox, you can define trusted pages using the computer name, IP address, or combinations of both. You can also use wildcards.

Procedure

1. Launch Mozilla Firefox.
2. Enter **about:config** in the address bar and press the Enter key. If a message is displayed, confirm it.
3. Enter **network.negotiate** in the **Filter** bar and press the Enter key.
4. Double-click **network.negotiate-auth.trusted-uris**.
5. Enter the computer name or IP address of the ARIS Server that has been configured for SSO and click **OK**.
6. Close and restart Mozilla Firefox.

If you want to use a stronger encryption than AES 128bit and if this is legally permitted in your country, replace the supplied JCE policy files of the JDK for ARIS Server with the **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 8** (**http://www.oracle.com/technetwork/java/javase/downloads/index.html**). This allows an unlimited key length.

If you cannot replace the policy files, but still want to use SSO, you must use a procedure that is supported by JDK for the encryption of Kerberos tickets (e.g., AES 128bit).

GOOGLE CHROME

Kerberos can be enabled by passing a comma-separated list of permitted URLs using the authentication server whitelist command line switch. For example pass in the following options that any URL ending in **mydomain.suffix.com** is permitted.

`--auth-server-whitelist="*.mydomain.suffix.com,*.suffix.com"`

Without the ***** prefix, the URL has to match exactly. MS Windows only: If the command line switch is not present, then the permitted list automatically contains all URLs of MS Internet Explorer local intranet zone.

6.2 Kerberos keys

You can configure Kerberos as required.

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.config	Configuration file Storage location of the configuration file for Kerberos. The file can be uploaded directly.	String	./config/Kerberos/krb5.conf
com.aris.umc.kerberos.debug	Debug output Specifies whether debug output is allowed for Kerberos operations.	true, false	
com.aris.umc.kerberos.kdc	KDC Specifies the fully qualified name of the central **K**ey **D**istribution **C**enter (**KDC**). This is usually the fully qualified host name of the LDAP server.	String	049bfs01.me.corp.softwareag.com
com.aris.umc.kerberos.keyTab	Key table Specifies the location of the keytab file that is used for Kerberos tickets. The file can be uploaded directly.	String	C:/safePlace/krb-umc.keytab
com.aris.umc.kerberos.realm	Realm Specifies the realm of Kerberos tickets. Fully qualified domain name in uppercase letters.	String	MY.CORP.SOFTWAREAG.COM

Key	Description	Valid input	Example
com.aris.umc.kerberos.servicePrincipalName	Principal Specifies the name of the user used for verifying Kerberos tickets. If Kerberos is used, each user, computer or service provided by a server must be defined as a principal.	String	MyLogin
com.aris.umc.kerberos.tenant	Default tenant Specifies the default tenant for a Kerberos-based login. Cross-tenant property that cannot be changed.	String	
com.aris.umc.kerberos.allowlocalusers	Allow local users Specifies whether the LDAP connection is mandatory for Kerberos-based login. If this option is enabled, Kerberos is used for the login of local users also.	true, false	

6.3 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 work with SSO have a valid user account in the related Directory Service (LDAP).
- The users exist in the ARIS Administration.
- ARIS Administration is configured against an LDAP server.
- 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 on client side.

CONFIGURATION OPTIONS IN ARIS ADMINISTRATION

You need to configure SSO for the servers.

Prerequisite

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

Procedure

1. Log in to the ARIS Administration.
2. Click the arrow next to your name.
3. Click **Administration**.
4. Click **Configuration**.
5. Switch to **User management**.
6. Select SAML.
7. To activate SSO, find the string

   com.aris.umc.saml.active

   Set this configuration key to true.
8. Define the ID of the service provider, e.g.

   `com.aris.umc.saml.service.provider.id=UMC@myhost`
9. Define the SSO POST binding endpoint of the identity provider, e.g.

   com.aris.umc.saml.identity.provider.sso.url=https://myidp/openam/SSOPOST/metaAlis/mytrust/idp

You activated Single Sign-On using SAML.

To configure SAML in detail please configure all SAML keys (page 22) in the ARIS Administration.

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 in the address bar:
   https://<SERVERNAME>/umc/rest/saml/metadata.xml?tenant=<TENANTID>
3. iptables -t nat -A PREROUTING -i <networt interface> -p tcp --dport <port n
4. Upload the file into your SAML identity provider.

Your system is configured to be used with Single Sign-On and SAML.

TROUBLESHOOTING

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

<Your installation folder>\ARIS9.8\server\bin\work\work_umcadmin_<size>\base\logs

Example

C:\SoftwareAG\ARIS9.8\server\bin\work\work_umcadmin_m\base\logs

6.4 SAML keys

Key	Description	Valid input
com.aris.umc.saml.active	Specifies if SAML-based login is allowed.	true, false
com.aris.umc.saml.identity.provider.id	ID of the identity provider.	String
com.aris.umc.saml.identity.provider.sso.url	SSO POST binding endpoint of the identity provider	String
com.aris.umc.saml.service.provider.id	ID of the service provider.	String
com.aris.umc.saml.signature.assertion.active	Specifies if SAML assertions must be signed.	true, false
com.aris.umc.saml.signature.request.active	Specifies if SAML authentication requests must be signed.	true, false
com.aris.umc.saml.signature.response.active	Specifies if SAML responses must be signed.	true, false
com.aris.umc.saml.truststore.location	Location of trust store file used to validate SAML assertions	File
com.aris.umc.saml.truststore.alias	Alias used to access the trust store	String
com.aris.umc.saml.truststore.password	Password used to access the trust store.	String
com.aris.umc.saml.truststore.type	Type of the trust store.	String
com.aris.umc.saml.login.mode.dn.active	Try login with full distinguished name instead of plain username.	true, false
com.aris.umc.saml.login.mode.keyword.active	Fallback to single keyword from distinguished name if login with full distinguished name fails.	true, false
com.aris.umc.saml.login.mode.keyword.name	Defines which part of the fully qualified name is to be used for log in.	String
com.aris.umc.saml.tenant	Default tenant used for SAML-based login.	String