

ARIS

ARIS SSO, LDAP,
KERBEROS, SAML, SCIM

VERSION 10.0 - SERVICE RELEASE 16
OCTOBER 2021

Document content not changed since release 10.0.14. It applies to the current version without changes.

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 - 2021 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

1	Configure single sign-on.....	1
2	Use LDAP	2
2.1	Add LDAP server	2
2.2	Test connection to an LDAP server	4
2.3	Customize LDAP	5
2.4	Customize ARIS for LDAP server operations	5
2.5	Configure secure communication	7
2.6	LDAP keys.....	9
2.7	Configure single sign-on (LDAP).....	31
2.7.1	Use Kerberos (LDAP).....	32
2.7.2	Use SAML (LDAP).....	37
2.8	Use ARIS with multiple LDAP systems.....	40
2.8.1	Kerberos (multiple LDAP systems)	40
2.8.2	SAML (multiple LDAP systems)	40
2.8.3	Single sign-on (multiple LDAP systems).....	40
2.8.4	WebDAV (multiple LDAP systems).....	41
2.8.5	ARIS Architect (multiple LDAP systems).....	41
2.8.6	Process Governance (multiple LDAP systems)	41
3	Use SCIM	42
3.1	Customize SCIM	42
3.2	SCIM keys.....	43
3.3	Configure single sign-on (SCIM).....	50
4	Customize Kerberos	52
5	Customize SAML	59
6	Legal information.....	72
6.1	Documentation scope.....	72
6.2	Support	73

1 Configure single sign-on

You can use single sign-on (SSO) together with an LDAP server or an SCIM server. The configuration of SSO using an LDAP server is described in chapter Use LDAP (page 31), the configuration of SSO using an SCIM server is described in chapter Use SCIM (page 50).

2 Use LDAP

2.1 Add LDAP server

LDAP enables information from a distributed, location-independent and hierarchical database in a network to be queried and modified.







You can use multiple LDAP servers with ARIS.

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

Prerequisite

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

Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
3. Click  **Configuration**.
4. Activate **User Management**.
5. Click the arrow next to **LDAP**.
6. Click **General settings**.
7. Click  **Edit**.
8. Enable **Use LDAP**.
9. Optional: Enable **Activate multiple LDAP integration** and confirm the **Property value change confirmation** dialog with **OK**.
10. Click  **Save**.
11. Click  **Add**. The **Add LDAP server** dialog opens.

12. Enter the following:

- ID of the LDAP server
- Display name of the LDAP server
- LDAP server URL
- LDAP server fallback URL
- User name of the user who has access to the LDAP content
- Password of this user
- Specify whether or not SSL should be used and in which mode
- Specify whether or not host names and certificates should be verified
- Specify the connection timeout
- Specify the read timeout

13. Click **Save**.

14. Click  **Save**.

You have added an LDAP server.

If you want to specify more than one LDAP server, proceed with step 10 of the procedure steps mentioned above.

2.2 Test connection to an LDAP server





LDAP enables information from a distributed, location-independent and hierarchical database in a network to be queried and modified.

You can use multiple LDAP servers with ARIS.

Prerequisite

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

Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
3. Click  **Configuration**.
4. Activate **User Management**.
5. Click the arrow next to **LDAP**.
6. Click the arrow next to the relevant LDAP server.
7. Click **Connection**.
8. Click  **Test connection**.

A message is displayed, whether or not the connection to the LDAP server specified is valid.

2.3 Customize LDAP

To customize (page 9) LDAP, please refer to the ARIS Connect online help (see chapter **Administrate ARIS Connect > Configure ARIS Connect > Set up user management > Customize LDAP settings**).






2.4 Customize ARIS for LDAP server operations

You can configure ARIS for LDAP server operations.

Prerequisite

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

Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
3. Click  **Configuration**.
4. Click **User management**.
5. Click the arrow next to **LDAP**.
6. Click **General settings**.
7. Click  **Edit**.
8. Enable **Use LDAP**. If you want to upload a configuration, ensure that you have disabled pop-up blockers in the browser.
9. Click **Truststore**. You must have generated a truststore file.
10. Click  **Upload**. The **Truststore** dialog opens. Select the truststore file you want to use.
11. Click the arrow next to the relevant LDAP server.
12. Configure the URL for the LDAP system. Click **Connection**.
13. Enter an ID, a name, and the URL in the **Server URL** field, for example:
`ldap://hggc.mycompany.com:3168`.
14. Configure the path to the backup system in the **Server URL (fallback)** field. This backup system takes over automatically if the LDAP server cannot be reached via its primary URL.

15. Click **Behavior**.
16. Enter the Path to the user group in the **Group search paths** field.
17. Enter the Path to the users in the **User search paths** field.

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

To disable the above behavior, enter **ignore** in the **Referral** field.

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

Optional: To ensure that the import of LDAP users is carried out despite any errors that might occur, for example, if names are redundant, click **Global settings > Advanced settings** and enable **Skip errors**.

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

You have configured ARIS for LDAP server operations.

2.5 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 LDAPS is activated.
- ARIS Administration trusts the LDAP server (the SSL certificate of the LDAP server or the certification authority is stored in the JRE database of trustworthy certificates).

STARTTLS

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





Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
3. Click  **Configuration**.
4. Click **User management**.
5. Click the arrow next to **LDAP**.
6. Click the arrow next to the relevant LDAP server.
7. Click **Connection**.
8. Click  **Edit**.
9. Configure the URL for the LDAP system. To do so, enter the URL as in the **Server URL** field, for example:
`ldap://hggc.mycompany.com:3168`.
10. Configure the path to the backup system in the **Server URL (fallback)** field. This backup system takes over automatically if the LDAP server cannot be reached via its primary URL.
11. Enable **Use SSL**.
12. Select **STARTTLS** from the **SSL mode** list.

13. ARIS must trust the LDAP server used. Therefore, we recommend that you use the LDAP server with a certificate signed by a public certification authority. If your certificate is signed by a public certification authority and stored in the list of trustworthy certificates of your JRE, you do not need to configure anything else.
14. Upload LDAP truststore file (page 5).

SSL

Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**.
3. Click  **Configuration**.
4. Click **User management**.
5. Click the arrow next to **LDAP**.
6. Click the arrow next to the relevant LDAP server.
7. Click **Connection**.
8. Click  **Edit**.
9. Configure the URL for the LDAP system. To do so, enter the URL as in the **Server URL** field, for example:
`ldap://hggc.mycompany.com:3168`
10. Configure the path to the backup system in the **Server URL (fallback)** field. This backup system takes over automatically if the LDAP server cannot be reached via its primary URL.
11. Enable **Use SSL**.
12. Select **SSL** from the **SSL mode** list.
13. ARIS must trust the LDAP server used. Therefore, we recommend that you use the LDAP server with a certificate signed by a public certification authority. If your certificate is signed by a public certification authority and stored in the list of trustworthy certificates of your JRE, you do not need to configure anything else.
14. Upload LDAP truststore file (page 5)

2.6 LDAP keys

You can customize LDAP as required.

GENERAL SETTINGS

Key	Description
com.aris.umc.ldap.active	Use LDAP Specifies whether or not the LDAP integration is enabled. Valid input true, false
com.aris.umc.ldap.multi.active	Activate multiple LDAP integration Specifies whether or not integration of multiple LDAP servers is to be activated. The default value is false . Valid input true, false
com.aris.umc.ldap.connection.count	Number of configured LDAP servers Displays the number of LDAP servers allowed. Valid input Integer Example 2

TRUSTSTORE

Key	Description
com.aris.umc.ldap.ssl.truststore.location	Truststore Specifies where to look for the truststore. Valid input String
com.aris.umc.ldap.ssl.truststore.password	Password Specifies the truststore password. Valid input String
com.aris.umc.ldap.ssl.truststore.type	Type Specifies the truststore type to be used. Valid input String

ADVANCED SETTINGS

Key	Description
com.aris.umc.ldap.debug	Debug output Specifies whether or not debug information for LDAP operations are output. Valid input true, false Example False
com.aris.umc.ldap.group.importParent.enabled	Import superior group Specifies whether the superior group is to be imported automatically when the group is imported. Valid input true, false Example False
com.aris.umc.ldap.user.importOnLogin	Import user at login Specifies whether an LDAP user is to be imported automatically during the login attempt. Valid input true, false Example False

Key	Description
com.aris.umc.ldap.sync.user.importGroups	<p>Import user groups when synchronizing</p> <p>Specifies whether additional user groups are to be imported during user synchronization.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.ldap.attribute.memberof.resolveOnFirstLogin	<p>Update group associations at login</p> <p>Specifies whether the memberOf attribute is read (true) or not (false). If the value of the property is true, the memberOf attribute is read and the referenced groups are automatically imported. The import of the groups occurs when a user from the group logs in for the first time.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.ldap.attributes.paging.enabled	<p>Use attribute value pagination</p> <p>Specifies whether a page break is to be inserted if the server-side limit for valid values is exceeded for attributes, for example, if more than 1,500 attribute values exist.</p> <p>Valid input</p> <p>true, false</p>

Key	Description
com.aris.umc.ldap.auth.only	<p>Prevent login of manually created users</p> <p>Specifies that only LDAP users may log in. This does not apply to the arisservice, guest, superuser, and system users.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.ldap.entity.cache.size	<p>Cache size</p> <p>Specifies the maximum number of LDAP entities that are cached during an import.</p> <p>Valid input</p> <p>Integer > 0</p> <p>Example</p> <p>3500</p>
com.aris.umc.ldap.connection.concurrent.timeout	<p>Pool wait time (in milliseconds)</p> <p>Specifies the maximum amount of time in milliseconds that a connection request may take if the maximum number of connections to the LDAP server was exceeded.</p> <p>Valid input</p> <p>Integer > 0</p>

Key	Description
com.aris.umc.ldap.connection.pool.size	<p>Pool size</p> <p>Specifies the maximum number of connections that are ready for reuse in a pool. The connection that was used last is discarded when the pool is full.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.umc.ldap.connection.pool.timeout	<p>Pool time (in milliseconds)</p> <p>Specifies the maximum amount of time that a connection remains in a pool. The connection is removed from the pool at the latest after this period of time. This is defined in milliseconds.</p> <p>Valid input</p> <p>Integer > 0</p>
com.aris.umc.ldap.sync.skipOnFault	<p>Skip errors</p> <p>Specifies whether the LDAP import ignores users or user groups for which errors occurred without showing an error message.</p> <p>Valid input</p> <p>True (without message), False (with error message)</p>

Key	Description
com.aris.umc.ldap.sync.members. searchBottomUp	<p>Use bottom-up method</p> <p>Specifies whether the bottom-up method (memberOf attribute) or the top-down method (hasMember attribute) is applied when associating users to user groups.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.ldap.sync.useDnAs Guid	<p>Use DN as GUID</p> <p>Specifies that the fully qualified name (distinguished name) is used as GUID.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

INDIVIDUAL LDAP SERVER

You can specify the properties of each individual LDAP server.

CONNECTION

Key	Description
com.aris.umc.ldap.connection.id plus the ID defined.	ID Specifies the unique ID of this specific LDAP connection. Valid input String
com.aris.umc.ldap.connection.name plus the ID defined.	Name Specifies the name of this specific LDAP connection. Valid input String
com.aris.umc.ldap.url	Server URL Specifies the URL of the LDAP server. Valid input String

Key	Description
com.aris.umc.ldap.backup.url	Server URL (fallback) Specifies the fallback URL of the LDAP server. This URL is only used if the server cannot be reached via its primary URL. Valid input String
com.aris.umc.ldap.service.user	User name Specifies the user name of the LDAP user. Valid input String Example arisldapservice
com.aris.umc.ldap.service.pwd	Password Specifies the password of the LDAP user. Valid input String
com.aris.umc.ldap.ssl	Use SSL Specifies if SSL is to be used. Valid input true, false

Key	Description
com.aris.umc.ldap.ssl.mode	SSL mode Specifies the SSL mode. Valid input String Example STARTTTLS
com.aris.umc.ldap.ssl.host.verification.active	Verify host names Specifies if an SSL host is to be verified. Valid input true, false
com.aris.umc.ldap.ssl.certificate.verification.active	Verify certificates Specifies whether an SSL certificate is to be verified. Valid input true, false
com.aris.umc.ldap.connection.concurrent	Simultaneous connections Specifies the maximum number of simultaneous connections to the same LDAP server. If additional connections are to be established, they are refused. Valid input Integer > 0

Key	Description
com.aris.umc.ldap.timeout	Connection timeout (in milliseconds) Specifies the duration after which the attempt to connect to the LDAP server is canceled. This is defined in milliseconds. Valid input Integer > 0
com.aris.umc.ldap.read.timeout	Read timeout (in milliseconds) Specifies the maximum amount of time that read access may take. This is defined in milliseconds. Valid input Integer > 0

ATTRIBUTE MAPPINGS

Key	Description
com.aris.umc.ldap.attribute.objectclass	objectClass Specifies the attribute that contains the object class. Valid input String Example objectClass
com.aris.umc.ldap.attribute.distinguishedname	DN Specifies the fully qualified name (distinguished name). Valid input String Example distinguishedName
com.aris.umc.ldap.attribute.guid	GUID Specifies the LDAP GUID. Valid input String Example Object GUID

GROUP ATTRIBUTE MAPPINGS

Key	Description	Valid input	Example
com.aris.umc.ldap.attribute.group.name	Name Specifies the group name. Valid input String Example Group name	String	Group name
com.aris.umc.ldap.attribute.hasmember	hasMember Specifies the attribute that references the members of a group. Valid input String Example hasMember	String	hasMember

Key	Description	Valid input	Example
com.aris.umc.ldap.group.attribute s.userdefined	User-defined Specifies a comma-separated list of LDAP attributes that are to be imported as user-defined attributes of a user group. Valid input String Example Description, operating system	String	Description, operating system

USER ATTRIBUTE MAPPINGS

Key	Description	Valid input	Example
com.aris.umc.ldap.attribute.user.name	<p>Name Specifies the user name of a user.</p> <p>Valid input String</p> <p>Example Fragment</p>	String	Fragment
com.aris.umc.ldap.attribute.user.firstname	<p>First name Specifies the first name of a user.</p> <p>Valid input String</p> <p>Example John</p>	String	John
com.aris.umc.ldap.attribute.user.lastname	<p>Last name Specifies the last name of a user.</p> <p>Valid input String</p> <p>Example Smith</p>	String	Smith

Key	Description	Valid input	Example
com.aris.umc.ldap.attribute.user.email	E-mail address Specifies the e-mail address of a user. Valid input String Example john.smith@softwareag.com	String	john.smith@softwareag.com
com.aris.umc.ldap.attribute.user.phone	Telephone number Specifies the telephone number of a user. Valid input String Example +491234567	String	+491234567
com.aris.umc.ldap.attribute.user.picture	Picture Specifies the picture of a user. Valid input Location of an image	Location of an image	

Key	Description	Valid input	Example
com.aris.umc.ldap.attribute.memberof	Member of Specifies the attribute that references the groups of a user. Valid input String Example memberOf	String	memberOf
com.aris.umc.ldap.user.attributes.userdefined	User-defined Specifies a comma-separated list of LDAP attributes that are to be imported as user-defined attributes of a user. Valid input String Example Description, operating system	String	Description, operating system

BEHAVIOR

Key	Description
com.aris.umc.ldap.group.objectclass	Group object class Object class of the LDAP groups. Valid input String Example Group
com.aris.umc.ldap.user.objectclasses	User object class Specifies the object class of the LDAP user. Valid input String Example Organizational unit

Key	Description
com.aris.umc.ldap.searchpath	<p>Search paths</p> <p>Specifies a semicolon-separated list of all LDAP search paths.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>OU\=stadt\,OU\=location\ OU\=employees\,DC\=my\,DC\=corp\ DC\=company\,DC\=com</p>
com.aris.umc.ldap.group.searchpath	<p>Group search paths</p> <p>Specifies a semicolon-separated list of all LDAP search paths for user groups. Overwrites the list of general search paths.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>OU\=distribution lists\,DC\=my,DC\=corp\,DC\=company\,DC\=com</p>

Key	Description
com.aris.umc.ldap.user.searchpath	<p>User search paths</p> <p>Specifies a semicolon-separated list of LDAP search paths for users. Overwrites the list of general search paths.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>OU\=employees\,DC\=my\,DC\=corp\ DC\=company\,DC\=com</p>
com.aris.umc.ldap.filter.group	<p>Group search filter</p> <p>Specifies the query filter for LDAP groups.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>(&(objectClass=role)(name=y*))</p>

Key	Description
com.aris.umc.ldap.filter.user	<p>User search filter</p> <p>Specifies the query filter for LDAP users.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>(&(sAMAccountName=*))</p>
com.aris.umc.ldap.recursion.depth	<p>Recursion depth</p> <p>Specifies the recursion depth that is to be used for nested groups and users.</p> <p>Valid input</p> <p>1 means one level, 0 means all</p> <p>Example</p> <p>1</p>
com.aris.umc.ldap.pagesize	<p>Page size</p> <p>Specifies the maximum number of entries that are loaded in a single LDAP query.</p> <p>Valid input</p> <p>Integer > 0</p>

Key	Description
com.aris.umc.ldap.referral	<p data-bbox="629 256 2078 363">Referrals Defines how referrals to other LDAP systems are processed.</p> <p data-bbox="629 368 2078 475">Valid input follow means that the referral is automatically</p> <p data-bbox="629 480 2078 595">Example ignore</p>

2.7 Configure single sign-on (LDAP)

If you are using Microsoft® Active Directory Domain Services, you can configure SSO (single sign-on). This allows users to work with all ARIS components as soon as they are logged in to the domain. Separate login to ARIS components is not required.

Please contact your LDAP administrator 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.

2.7.1 Use Kerberos (LDAP)

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.

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 IN ARIS ADMINISTRATION



You need to configure SSO for the servers.

Procedure

1. Start ARIS Connect.
2. Click  **Application launcher** >  **Administration**. The **Administration** view opens.
3. Click  **Configuration**.
4. Click **User management**.
5. Click the arrow next to **Kerberos**.
6. Activate the **General** configuration category.

If you do not have a Kerberos configuration file, take the **kbr5.conf** from your installation media under **Add-ons\Kerberos**. Name it, for example, **krb5.conf**, add the following lines, and adjust the configuration to meet your requirements.

```
[libdefaults]
default_tgs_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.

You can use Kerberos with multiple LDAP systems (page 40).

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.

2.7.2 Use SAML (LDAP)

SAML (**S**ecurity **A**ssertion **M**arkup **L**anguage) is an XML framework for exchanging authentication and authorization information. SAML provides functions to describe and transfer security-related information.

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

- 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 meta data XML file if SAML is enabled.

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 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  **Application launcher** >  **Administration**. The **Administration** view opens.
3. Click  **Configuration**.
4. Click **User management**.
5. Click the arrow next to **SAML**.
6. Click **General**.
7. Click  **Edit**.
8. Enable **Use SAML**.
9. Enter the ID of the identity provider in the **Identity provider ID** field.
10. Enter the ID of the service provider in the **Service provider ID** field.
11. Enter the end point of the identity provider that is used for single sign-on in the **Single sign-on URL** field.
12. Enter the end point of the identity provider that is used for single log-out in in the **Single logout URL** field.

You have configured SSO using SAML in ARIS Administration. If you use multiple LDAP systems (page 40), the user names must be unambiguous through all LDAP systems. Otherwise no SSO is possible.

You can use SAML with multiple LDAP systems (page 40).

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_umcadmin_<size>\base\logs

Example

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

2.8 Use ARIS with multiple LDAP systems

ARIS supports the use of multiple LDAP systems. 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 are going to use multiple LDAP systems with already existing data, for example, attributes, all data must be renewed first.
- Each LDAP server must have a unique ID to identify the server to be used at user login and for user group names.
- The format of the ID must not exceed five characters
- The user or user group names are prefixed with the server ID in the following format: LDAP1\user1, LDAP2\user group name.

If the user name is defined in the format shown above, the users must enter the prefix when logging in.

2.8.1 Kerberos (multiple LDAP systems)

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

When using multiple LDAP systems, the **Ignore realm from service ticket** property under **Kerberos -> Advanced Settings** must be enabled.

2.8.2 SAML (multiple LDAP systems)

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.

2.8.3 Single sign-on (multiple LDAP systems)

If users have the same login ID in different LDAP servers, the Single sign-on (page 31) login fails. Users must enter their passwords manually instead.

2.8.4 WebDAV (multiple LDAP systems)

The WebDAV protocol provides a framework for users to create, change and move documents on a server. The most important features of the WebDAV protocol include the maintenance of properties about, for example, an author or modification date.

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

2.8.5 ARIS Architect (multiple LDAP systems)

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

Example

Search for a user in ARIS Architect for user **LDAP1\user1**, the user is found.

Search for user **user1** without the prefix, the user is not found.

2.8.6 Process Governance (multiple LDAP systems)

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

3 Use SCIM

3.1 Customize SCIM

To customize (page 43) SCIM, please refer to the ARIS Connect online help (see chapter **Administrate ARIS Connect > Configure ARIS Connect > Set up user management > Customize SCIM settings**).

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 (page 43) to the SCIM administrator.

3.2 SCIM keys

You can configure SCIM as required.

GENERAL

Key	Description
com.aris.umc.scim.active	<p>Use SCIM</p> <p>Enables SCIM support for User Management.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
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> <p>Valid input</p> <p><loadbalancerurl>/umc/scim/v2/{tenant}</p>

Key	Description
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> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>
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> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>True</p>
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> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>365</p>

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> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>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> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>	True, False	False

Key	Description	Valid input	Example
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> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>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> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>	True, False	False

SCIM CLIENT

Key	Description	Valid input	Example
com.aris.umc.scim.connection.enabled	<p>Provisioning</p> <p>Specifies whether the synchronization of users or user groups for the configured application is enabled. The default value is false.</p> <p>Provisioning and re-provisioning from the SCIM client</p> <p>A valid re-provisioning scenario is that users can be moved from the SCIM client to the SCIM server using the SCIM provisioning user interface. You must use the SCIM provisioning user interface to remove users from the SCIM server. You must use the SCIM provisioning user interface to add these users again to the SCIM server.</p> <p>An invalid re-provisioning scenario is that users can be moved from the SCIM client to the SCIM server using the SCIM provisioning user interface. If the administrator logs into the SCIM server itself and deletes all users from the SCIM server but the list of associated users is still maintained in the SCIM client system. This system does not know that users have been deleted from the SCIM server. Therefore, if the administrator wants to delete users directly in the server, the administrator must remove these users from the SCIM provisioning interface and add these users again using the SCIM provisioning interface. The default value is false.</p>	True, False	False

Key	Description	Valid input	Example
com.aris.umc.scim.connection.name	<p>Connection name</p> <p>Specifies the connection name used for identifying the application with which the user accounts are synchronized.</p>	String	myconnection
com.aris.umc.scim.connection.provision.mode	<p>Provisioning mode</p> <p>Specifies whether the creation and synchronization of user accounts based on user and group assignments is performed manually or automatically. The default value is Manual.</p>	Manual, Automatic	Manual
com.aris.umc.scim.connection.url	<p>Connection URL</p> <p>Specifies the connection string used to communicate with the SCIM services.</p>	URL	https://myserver.com
com.aris.umc.scim.connection.secret.token	<p>Secret token</p> <p>Is used to access the SCIM services to synchronize the user accounts.</p>	String	37283011-bd3e-4efe-8ed4-5f207b094453
com.aris.umc.scim.connection.provision.options	<p>Objects for provisioning</p> <p>Specifies which objects are synchronized. The default value is true.</p>	True, False	True
com.aris.umc.scim.connection.user.provision.actions	<p>Supported user actions</p> <p>Specifies what user actions are supported. The default value is true.</p>	True, False	True

Key	Description	Valid input	Example
com.aris.umc.scim.connection.group.provision.actions	Supported group actions Specifies what group actions are supported. The default value is true .	True, False	True
com.aris.umc.scim.connection.user.email.as.username	Use e-mail address as the user name Specifies that the e-mail address is used as the user name. If you want to use this option, the e-mail addresses must be unambiguous. Otherwise, all actions performed for users or user groups will fail. The default value is false .	True, False	False

3.3 Configure single sign-on (SCIM)

You can use single sign-on (SSO) using SCIM. Separate login to ARIS components is not required. The **S**ystem for **C**ross-Domain **I**ntity **M**anagement 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 43).

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  **Application launcher** >  **Administration**. The **Administration** view opens.
3. Click  **Configuration**.
4. Click **User management**.
5. Click the arrow next to **SCIM**.
6. Click **General**.
7. Click  **Edit**.
8. Enable **Use SCIM**.
9. Click  **Save**.

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

4 Customize Kerberos

Kerberos is a network authentication, allowing nodes to communicate using an invisible network and to securely make their identity known to each other. Kerberos is the recommended method for user authentication in Microsoft® Windows networks. In addition, it is widely used with Linux operating systems and is designed for use with all major platforms.

The prerequisites for a Kerberos integration are the following:

- **Server**
 - Users 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 supports a Kerberos-based authentication and has been configured accordingly (page 32).

To customize Kerberos, please refer to the ARIS Connect online help (see chapter **Administrate ARIS Connect > Configure ARIS Connect > Set up user management > Customize Kerberos settings**). If you are going to migrate data from ARIS 9.8.7 or later, customize Kerberos after the migration. The Kerberos settings of the former ARIS version will overwrite the current settings during data migration.

You can use Kerberos for single sign-on (page 32).

CREATING A KEY TABLE FILE

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 in the console:

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

DISPLAY EXISTING KEY TABLE FILE

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

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

KERBEROS KEYS

You can configure Kerberos as required.

You can change properties that are highlighted as cross-tenant properties only by using the 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
com.aris.umc.kerberos.active	<p>Use Kerberos</p> <p>Specifies whether a Kerberos-based login is allowed.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.kerberos.kdc	<p>KDC</p> <p>Specifies the fully qualified name of the central Key Distribution Center (KDC). This is usually the fully qualified host name of the LDAP server.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>mykdc.mydomain.com</p>
com.aris.umc.kerberos.realm	<p>Realm</p> <p>Specifies the realm of Kerberos tickets. Fully qualified domain name in uppercase letters.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>MY.CORP.SOFTWAREAG.COM</p>

Key	Description
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> <p>Valid input</p> <p>String</p> <p>Example</p> <p>MyLogin</p>
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> <p>Valid input</p> <p>String</p> <p>Example</p> <p>C:/safePlace/krb-umc.keytab</p>

Key	Description
com.aris.umc.kerberos.config	<p data-bbox="631 258 2078 300">Configuration file</p> <p data-bbox="631 306 2078 354">Storage location of the configuration file for Kerberos.</p> <p data-bbox="631 360 2078 408">The file can be uploaded directly.</p> <p data-bbox="631 414 2078 462">Valid input</p> <p data-bbox="631 469 2078 517">String</p> <p data-bbox="631 523 2078 571">Example</p> <p data-bbox="631 577 2078 625">./config/Kerberos/krb5.conf</p>

ADVANCED SETTINGS

Key	Description
com.aris.umc.kerberos.debug	Debug output Specifies whether debug output is allowed for Kerberos operations. Valid input true, false
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. Valid input true, false
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 . Valid input true, false

Key	Description
com.aris.umc.kerberos.tenant.	<p data-bbox="631 258 2078 295">Default tenant</p> <p data-bbox="631 316 2078 400">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.</p> <p data-bbox="631 469 2078 505">Valid input</p> <p data-bbox="631 523 2078 560">true, false</p>

5 Customize SAML

SAML (**S**ecurity **A**ssertion **M**arkup **L**anguage) is an XML framework for exchanging authentication and authorization information. SAML provides functions to describe and transfer security-related information.

SAML must be enabled for ARIS.

Enter the following URL to receive the meta-data that you can hand-over to your identity provider or provide the URL to your identity provider:

`http://<your ARIS server>/umc/rest/saml/metadata.xml`

The administrator of the identity provider provides you a XML file with the relevant. Usually, this is an XML file containing all relevant information about the identity provider. If such a file does not exist, please make sure to get at least the following information from the SAML administrator:

- Identity provider ID
- Service provider ID
- Single sign-on URL
- X.509 Certificate (in case assertions are signed)

The provided information should then be specified in ARIS.

To customize SAML, please refer to the ARIS Connect online help (see chapter **Administrate ARIS Connect > Configure ARIS Connect > Set up user management > Customize SAML settings**).

You can use SAML with single sign-on together with an LDAP server (page 37) or an SCIM server (page 42).

SAML KEYS

You can configure SAML as required.

You can change properties that are highlighted as cross-tenant properties only by using the 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
com.aris.umc.saml.active	<p>Use SAML</p> <p>Specifies whether an SAML-based login is allowed.</p> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
com.aris.umc.saml.binding	<p>Binding</p> <p>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.</p> <p>Example</p> <p>POST</p>

Key	Description
com.aris.umc.saml.identity.provider.id	Identity provider ID Specifies the ID of the identity provider. Valid input String
com.aris.umc.saml.service.provider.id	Service provider ID Specifies the ID of the service provider. Valid input String
com.aris.umc.saml.identity.provider.sso.url	Single sign-on URL Specifies the end point of the identity provider that is used for single sign-on.
com.aris.umc.saml.identity.provider.logout.url	Single logout URL Specifies the end point of the identity provider that is used for single log-out.

SIGNATURE

Key	Description
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> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
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> <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>

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

KEYSTORE

Key	Description
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. Valid input String
com.aris.umc.saml.keystore.password	Password Specifies the password that is used to access the keystore. Valid input String
com.aris.umc.saml.keystore.type	Type Specifies the type of the keystore to be used. The keystore type can be selected from a list. Valid input String Example JKB

TRUSTSTORE

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

USER ATTRIBUTES

Key	Description
com.aris.umc.saml.attribute.fname	First name Specifies the attribute name to be used for reading first names from a SAML assertion. Valid input String Example John
com.aris.umc.saml.attribute.lname	Last name Specifies the attribute name to be used for reading last names from a SAML assertion. Valid input String Example 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. Valid input String Example jd@company.com

Key	Description
com.aris.umc.saml.attribute.phone	<p>Telephone number</p> <p>Specifies the attribute name to be used for reading phone numbers from a SAML assertion.</p> <p>Valid input</p> <p>Integer</p> <p>Example</p> <p>01234567</p>
com.aris.umc.saml.attribute.memberof	<p>Member of</p> <p>Attribute that references the groups of a user.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>Main group</p>
com.aris.umc.saml.attribute.userdefined	<p>User-defined</p> <p>Comma-separated list of attributes to be imported as user-defined attributes of the user.</p>

ADVANCED SETTINGS

Key	Description
com.aris.umc.saml.login.mode.dn.active	<p>Login using DN</p> <p>Specifies whether login is to be tried using the fully qualified name instead of the user name.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.saml.login.mode.keyword.active	<p>Decompose DN</p> <p>Specifies whether the fully qualified name is to be decomposed.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.saml.login.mode.keyword.name	<p>Keyword</p> <p>Specifies which part of the fully qualified name is to be used for login.</p> <p>Valid input</p> <p>true, false</p>
com.aris.umc.saml.auth.context.class.refs	<p>Authentication context classes</p> <p>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.</p>

Key	Description
com.aris.umc.saml.auth.context.comparison	<p>Authentication context comparison</p> <p>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.</p> <p>Valid input</p> <p>String</p>
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> <p>Valid input</p> <p>String</p>

Key	Description
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. <p>Valid input</p> <p>true, false</p> <p>Example</p> <p>False</p>
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> <p>Example</p> <p>60</p>
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>

Key	Description
com.aris.umc.saml.assertion.ttl	<p>Assertion lifetime (in seconds)</p> <p>Specifies the maximum lifetime of a SAML assertion in seconds.</p> <p>Example</p> <p>10</p>
com.aris.umc.saml.service.provider.assertion.consumer.url.override	<p>Assertion Consumer Service URL</p> <p>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/initssso. If no specification is made, the URL is derived from the HTTP request.</p>
com.aris.umc.saml.tenant	<p>Default tenant</p> <p>Specifies the default tenant that is to be used for the SAML-based login.</p> <p>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.</p> <p>Valid input</p> <p>String</p> <p>Example</p> <p>default</p>

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 websites.

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.

SOFTWARE AG EMPOWER PORTAL

You can find documentation on the Software AG Documentation website (<https://empower.softwareag.com/>). The site requires credentials for Software AG's Product Support site **Empower**. If you do not yet have an account for **Empower**, send an e-mail to empower@softwareag.com with your name, company, and company e-mail address and request an account.

If you have no account, you can use numerous links on the TECHcommunity website. For any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory and give us a call.

TECHCOMMUNITY

On the **TECHcommunity** website, you can find documentation and other technical information:

- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Access articles, code samples, demos, and tutorials.
- Find links to external websites that discuss open standards and web technology.
- Access product documentation, if you have **TECHcommunity** credentials. If you do not, you will need to register and specify **Documentation** as an area of interest.

EMPOWER (LOGIN REQUIRED)

If you have an account for **Empower**, use the following sites to find detailed information or get support:

- You can find product information on the Software AG Empower Product Support website.
- To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the Knowledge Center.
- Once you have an account, you can open Support Incidents online via the eService section of Empower.
- To submit feature/enhancement requests, get information about product availability, and download products, go to Products.

SOFTWARE AG MANAGED LEARNINGS

Get more information and trainings to learn from your laptop computer, tablet or smartphone. Get the knowledge you need to succeed and make each and every project a success with expert training from Software AG.

If you do not have an account, register as a customer or as a partner.