

Access Information List (AIL)

[\[Background \]](#) [\[Use Cases \]](#) [\[API \]](#) [\[See Also.. \]](#)



- IDMS as IDP is **NOT** responsible for user roles/groups creation for the user based on service provider application. The service provider application is responsible for managing user roles/groups for its users and IDMS will only store and assert the data
- IDMS as IDP **IS** responsible for managing the application list user accesses based on the user journey
- IDMS AIL capability is available on all the **supported protocols**
- IDMS recommends all service provider applications to review all their new AIL user roles/groups they want to use or updates to them with IDMS AIL governance team. Please make sure the AIL user roles/groups that you want to use are approved before using them with IDMS AIL APIs. For new service provider applications integrating with IDMS, please work with your application onboarding champion to get your AIL values approved by IDMS AIL governance team

Background

IDMS as Identity Provider (IDP) is responsible for managing a global persona of the user. As part of this responsibility IDMS manages a global role of the user. However many of the service provider applications that consume IDMS services may require application specific roles to drive granular access within their applications or target specific content. This will require service provider applications to intercept the user flow after authentication and then based on user enforce granular access. This may lead to performance issue and potentially bad user experience. Also some of these applications are SAAS based and have strict boundaries on what is customizable. To better serve all of these applications IDMS has built Access Information List (AIL) capability that stores information about user roles for each of the service provider applications as well the list of applications using IDMS that the user accesses. IDMS can then assert this information as response during login process to the service provider stand alone or SAAS applications and the applications then can process the user role and grant access without having to run additional queries thereby improving performance. IDMS only responsible for the assertion and storing of the service provider application user roles for the user. The service provider application is responsible for managing the user role for its users.

IDMS has two features as part of its AIL capability

- **AIL Applications**
 - Provides a list of service provider applications on IDMS the user has chosen to access
 - Application name and Application ID which is a hash created by IDMS and shared with application during Application on-boarding process
 - IDMS will own creation of this record (Current implementation is service provider application based)
 - IDMS will assert this value as CSV or return as CSV in all IDMS APIs that return user information
 - AIL application values can be used as a value proposition to seamless UX program where user can be shown all his/her applications access in one place on a dashboard
- **AIL Programs**
 - Provides a list of user roles/groups that service provider applications have assigned to the user
 - This list can contain multiple roles/group for each user for each service provider application as an user can choose to access multiple service provider applications using IDMS as IDP
 - Service provider application will own creation of these records for the user
 - IDMS will assert these values as CSV or return as CSV in all IDMS APIs that return user information

What is Standardized Master List (SML)?

Standardized Master List (SML) is a list of unique approved user roles for the service provider applications to use with IDMS AIL. This prevents duplication of the user role thereby increasing data quality and performance during querying or parsing. The main problem this solves is interpretation of a role by different service provider applications. For example a service provider application A wants to denote an internal user as "Employee", the same role can be defined by another service provider application as "Internal_user". These two roles have the same function but different AIL values. Another example is "End User" vs "End-user" or "Consumer". They all mean the same. SML will eliminate such conflicts keeping the data consistent across all service provider applications using IDMS. IDMS AIL governance team is responsible for managing the conflicts along with IDMS Data Quality lead. Also if new values need to be added they need to be presented and approved by AIL governance team




- This is a future enhancement. The current implementation allows any service provider application to create any user role for the user in IDMS AIL

AIL Governance

AIL governance is a process that regulates what values are standardized for applications to using IDMS AIL capability. This governance applies to both AIL features namely application names/hash and service provider defined user roles/groups. The AIL governance team consists of IDMS Product Owner, IDMS Data quality lead and IDMS Engineering lead. IDMS Data quality lead's responsibility is to review the data in **SML** and provide a solution in case of conflicts to both IDMS engineering team and the service provider application team. If the service provider application wants to add a new AIL user role/group value they need to present the use case to AIL governance team in **IDMS CRB(Change Request Board)** and seek approval. If this is not done this may result in bad user experience (see [use cases](#) below for more details). AIL application value for service provider application integrating with IDMS will be handed over to application as part of the *Integration Contract* during application on-boarding process.

AIL Response Examples -

SAML Example -	OIDC Example -
<pre><saml:Attribute Name="AIL Programs" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname format:unspecified"><saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:anyType">User,Power User,BMS Partner,EcoXpert Registered </saml:AttributeValue> </saml:Attribute></pre>	 <p>OIDC AIL ...Token.txt</p>

Use Cases

Use Case	User Flow	Outcome
Self Registration - User	<ul style="list-style-type: none"> User clicks "Register" on the IDMS provided branded login page for the service provider application OR User clicks on a deep link on a service provider application page 	<ul style="list-style-type: none"> See Registration use cases for the user flow and authentication After user activates his/her registration, IDMS will add an AIL Application entry for that user for the service provider application he/she registered for When the user lands on service provider application page IDMS sends all the information about the user in the assertion or openid connect token. The service provider application also choose to call any of the IDMS user APIs to get user information as well Then the service provider application can assign approved AIL programs value which is namely a user role or group to the user using IDMS AIL APIs The service provider application can then enforce further granular access to the user during next login or re-query the user information using IDMS APIs and enforce it real time
User accessing multiple SE service provider applications after initial registration WITHOUT an active IDMS session	<ul style="list-style-type: none"> User has successfully registered and activated his /her registration User comes to IDMS application specific branded login page User enter his credentials 	<ul style="list-style-type: none"> See Authentication use cases for the user flow IDMS will add an AIL Application entry for that user for the service provider application he/she is currently accessing and redirects user to the service provider application page and sends all the information about the user in the assertion or openid connect token. The service provider application also choose to call any of the IDMS user APIs to get user information as well Then the service provider application can assign approved AIL programs value which is namely a user role or group to the user using IDMS AIL API The service provider application can then enforce further granular access to the user during next login or re-query the user information using IDMS APIs and enforce it real time
User accessing multiple SE service provider applications after initial registration WITH an active IDMS session	<ul style="list-style-type: none"> User has been successfully authenticated by IDMS on a service provider application User now has a valid IDMS session User then accesses another service provider application using IDMS 	<ul style="list-style-type: none"> See SSO/SLO use cases for the user flow IDMS will intercept SSO and add Application AIL and seamlessly redirect the user to the service provider application landing page

Service provider application assigning a Non Approved AIL Programs value for the user post login	<ul style="list-style-type: none"> • User has successfully registered and activated his /her registration • User comes to IDMS application specific branded login page • User enter his credentials 	<ul style="list-style-type: none"> • When the user lands on service provider application page after IDMS authentication , IDMS send all the information about the user in the assertion or openid(OIDC) connect token. The service provider application also choose to call any of the IDMS user APIs to get user information as well • Then the service provider application assigns AIL programs value which is namely a user role or group to the user using IDMS AIL API but one <i>which has not been approved</i> by IDMS AIL Governance team • IDMS allows the the service provider application to create the new AIL program entry even though it is not approved so as to not to interrupt user experience.The service provider application can then enforce further granular access to the user during next login or re-query the user information using IDMS APIs and enforce it real time • Behind the scenes IDMS flags this entry in the database for review by the IDMS data quality lead • The IDMS data quality lead reviews the flagged entries once every week and then works with AIL governance team and service provider application team to either resolve the conflict or accepts the new AIL programs entry, presents it to IDMS CRB and after getting it approved adds it to the SML <ul style="list-style-type: none"> • In case of conflict, the IDMS Data quality lead will provide alternate AIL programs value from SML to the service provider application team and once the agreement is reach will update all the user AIL Programs data in IDMS and service provider application will need to do the same on their end • The timing of this will be coordinated by IDMS Data quality lead because if the data update is out of sync in case of conflict it can result in bad user experience
--------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

API

Exposed APIs	Supported APIs
GetUserAILbyFederation ID - Technical user token needed UpdateUserAIL - Technical user token needed	Getuserprofile - User access token needed GetuserbyApplication - Technical user token needed GetAllUsersbyApplication - Technical user token needed CreateUser - Technical user token needed UpdateuserProfile - User access token needed



- *IDMS send all AIL values as part of assertion or openid connect token during the login process.. The service provider applications can use this data to provide further granular access to the user without having to call IDMS AIL APIs*
- *All IDMS User APIs return AIL data*
- *If applications need ONLY AIL information without user information or user session then they need to use either GetUserAILbyFederationID API. This is restricted use API and should be used in special cases only.*

See Also..

[Registration](#), [Authentication](#), [Third Party Authentication](#), [Progressive Profile](#), [API as service](#)