# IDM AS A SERVICE

**Chetana Tukkoji [1],M Sahithi Prasanthi [2],Ch Ahalya [3],J Rojee Rao[4]**
[1]Assistant Professor, Dept. of Computer Science and Engineering, GITAM Deemed to be University, Bangalore
[2,3,4] Dept. of Computer Science and Engineering, GITAM Deemed to be University, Bangalore

## ABSTRACT:

IDM is a structure for business process that makes the management and accessing easier and efficient. IDM enables the authorized user to access the required information. It is a process of controlling information about users. Identity is provided for the user access. It also provides the management of how, who the information can be accessed and modified. Forgerock is one of the software companies that implement the IDM which develops products for cloud customers, enterprise environment. This paper elaborates the usage of Forgerock IDM for the centralized user management.

**Keyword:** Forgerock **, IDM, Cloud**

## I. INTRODUCTION

IDM stands for identity and access management. It can be used for single sign-in i.e., once the user logs in, the user's information is provided with an identity and security which helps to maintain confidentiality, integrity, authenticity and non repudiation. The user's access is being monitored in such a way that the user follows a particular pattern that is being referred as user's identity. Forgerock is a platform which contains many components such as OpenDJ, OpenAM, OpenIDM, OpenIG and so on[8][9][10]. OpenDJ is the Directory Server or a database used to store user's details. OpenAM provides authentication and authorization for the users. OpenIDM provides identity and access management. OpenIG is the identity gateway that provides security to the user's information.

## II. EXISTING SYSTEM

The current system exists only with the components in the Forgerock but not the user management. It becomes difficult to maintain and retrieve the data efficiently using present technology[1][8][9][10]. As the component contains maximum number of users the retrieval of data becomes difficult, so retrieval of user's information from any components becomes a great challenge[2].

## III. PROBLEM STATEMENT

To integrate the various components of Forgerock to facilitate the features of centralized user management and single sign-in. As the previous system is limited only to the little functionalities to single sign-on. Centralized user management would help to manage the user information by integrating components of Forgerock with one another.

## IV. OBJECTIVES

The objective of this paper is to provide services based on users information with the help of Forgerock using IDM(Identity Management) as a service. Centralized user management is provided for the users with the components of the Forgerock by integrating each of them with one another. The existing system has only the components in the Forgerock but the centralized user management is not provided. Centralized user management helps to keep track of user information in a secured fashion.

## V. SYSTEM ARCHITECTURES

### 1. Forgerock Components

Fig 1. Elaborates various components of the Forerock. Forgerock has four main components.

a. OpenDJ
b. OpenAM
c. OpenIDM
d. OpenIG

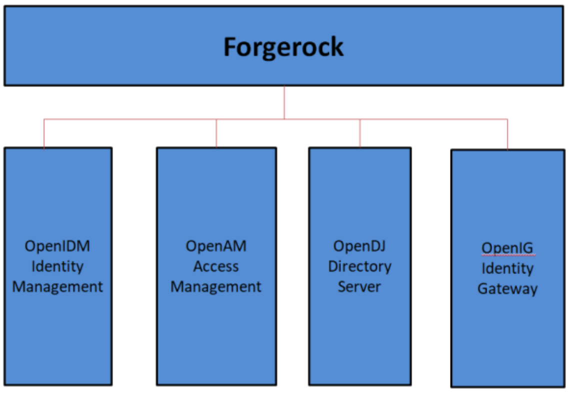


Fig 1. Forgerock components

### a. OpenDJ

OpenDJ is an open source software. It uses LDAP(Light weight directory access protocol) Directory server. OpenDJ is used for storage. It provides the following services:

- Performance, Scalability and High availability
- Password policy and schema management
- Active directory synchronization
- Identity replication

### b. OpenAM

It is an open source software solution for authentication and authorization. It helps to validate the entered details of the user with the help of OpenDJ database that indicates that the OpenDJ and OpenAM are interconnected. It provides the following services:

- Authentication
- Authorization
- Entitlement management
- Federation
- Single sign-in
- Adaptive authentication(risk management)

### c. OpenIDM

It is open source software that provides identity and access management for the users in order to access and retrieves data easily. It provides the following services:

- User provisioning
- User self service
- Synchronization
- Reconciliation
- Workflow management

### d. OpenIG

It is an identity gateway that provides security for the user's information that is being accessed by the user. It provides the following services:

- API security
- Mobile security
- Legacy app security
- Web services security
- Password capture and replay

## 2. Forgerock Architecture

The Fig 2 elaborate the architecture of Forgerock which covers the entire workflow of the user login and access management.

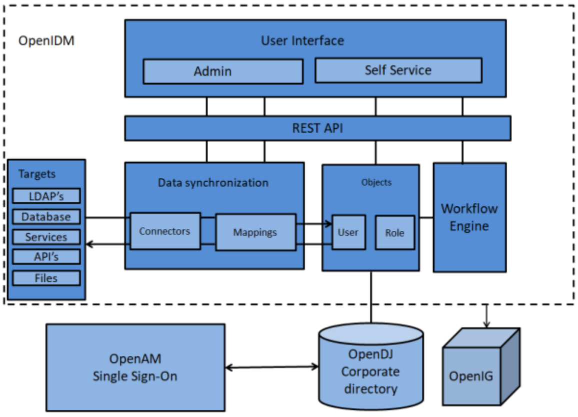


Fig 2. Forgerock architecture

In OpenIDM, the user registers his/her information for sign up.During the authentication process, once the user key in the details , it contacts with the OpenDJ for the verification of the details in database, if it exists the user will be allowed to access through OpenAM in a secured way via OpenIG.If the user crendentials are not verified the permission for the user to access is denied. After accessing the user can access the information depending up on his entitlements.

## 3. Provisioning

The integration of components is done by using connectors. LDAP connector is used as an interface for communicating between the components. LDAP is a public standard that provides maintenance and accessto dispense directories such as network by an Internet Protocol (IP) network. LDAP servers are free to use open source projects and packages. LDAP connector is the only source used in this paper in order to integrate. Several steps are used to integrate the components of Forgerock.

The connector needs to be added once the installation and configuration of OpenIDM and OpenDJ are successfully done. Configuration of connector is needed to find the list of users, both of OpenIDM and OpenDJ. The configuration of connector is elaborated in figures 3,4 and 5

Once the user logs in to the OpenIDM the dashboard appears and there an option called "**Add Connectors**" needs to be selected.

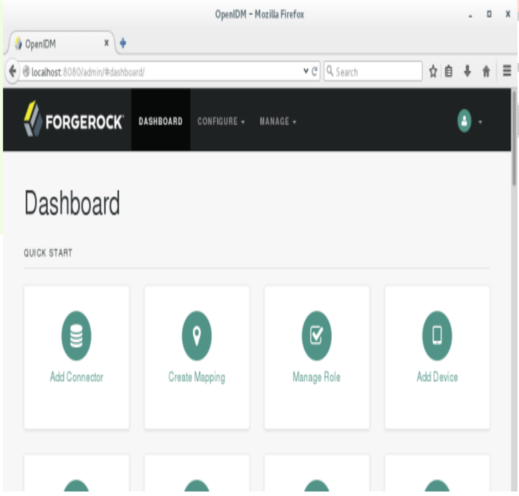
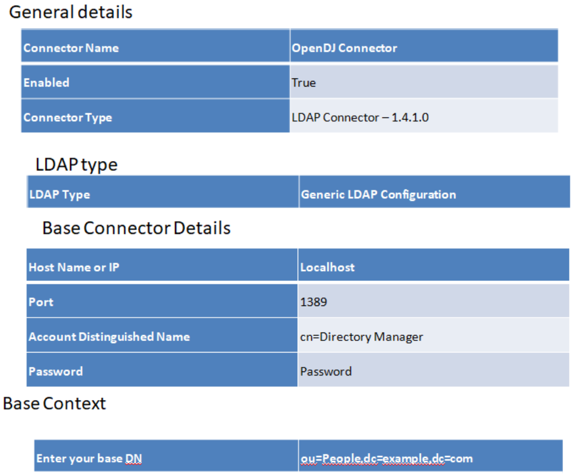


Fig 3. Dashboard of OpenIDM

The connector details should be filled as follows:



General details

| Connector Name | OpenDJ Connector |
|---|---|
| Enabled | True |
| Connector Type | LDAP Connector – 1.4.1.0 |

LDAP type

| LDAP Type | Generic LDAP Configuration |
|---|---|

Base Connector Details

| Host Name or IP | Localhost |
|---|---|
| Port | 1389 |
| Account Distinguished Name | cn=Directory Manager |
| Password | Password |

Base Context

| Enter your base DN | ou=People,dc=example,dc=com |
|---|---|

Fig 4. Connector details

Once the connector is successfully added, then the connector is in active state. After the connector comes to an active state, the mappings of attributes of source and target are linked. The mappings are done in such a way that the attribute fields of the users are between the source and target are the same. The link qualifier can either be a default or with a specific link. If the link qualifier is default, it links with the random attribute fields of the user else, it links with the attribute fields with that particular user.

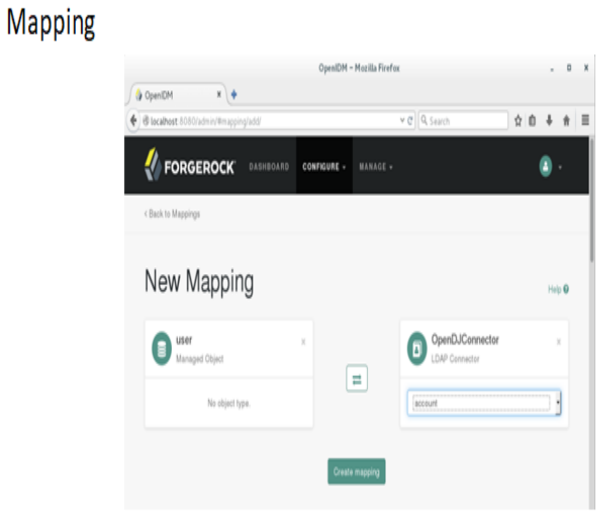
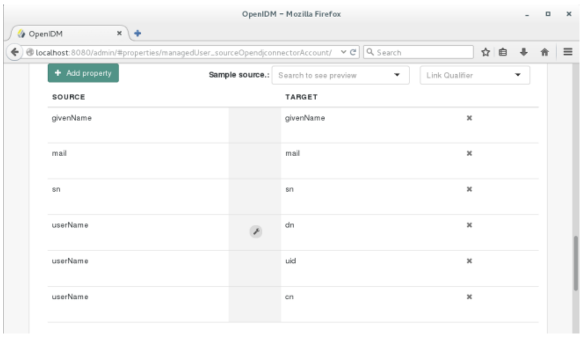


Fig 5.Mapping

Here the base context refer to the main root where it contains a domain called example com. The root is the people where it contains many number of users under the same domain with different set of attribute field values, each user has its own properties and identity provided with a specified object.

Mapping is done between source i.e., OpenIDM users with the Target i.e., LDAP connector i.e., the interface of OpenDJ in order to map. Mapping is done by linking each attribute field of source and target with the same name.


OpenIDM – Mozilla Firefox
OpenIDM
localhost:8080/admin/#properties/managedUser_sourceOpendjconnectorAccount/
Search
+ Add property
Sample source.:
Search to see preview
Link Qualifier

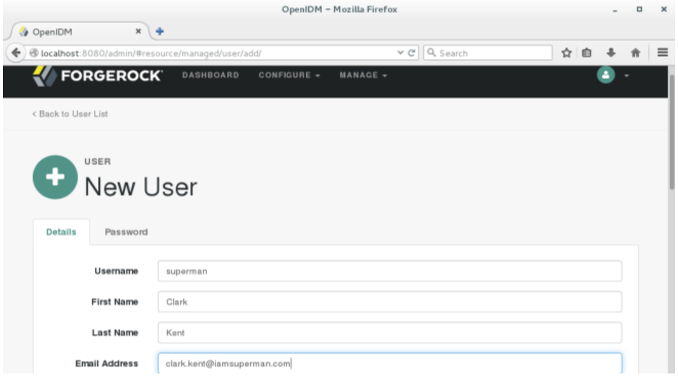
| SOURCE | TARGET | |
|---|---|---|
| givenName | givenName | × |
| mail | mail | × |
| sn | sn | × |
| userName | dn | × |
| userName | uid | × |
| userName | cn | × |

Fig 6. Linking of Source and Target Attributes

The following steps elaborate the provisioning of the users as shown in fig 9:

- Click on the Association tab. Under Association Rules,
- Click on the dropdown list and choose Correlation Queries.

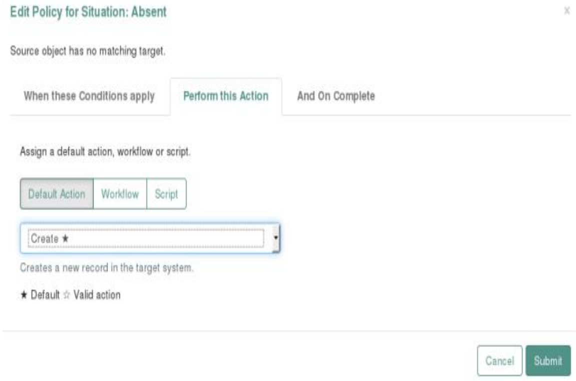
- Go to Expression Builder, add the additional fields mail and uid. Select “Any of the following fields” from the dropdown list.
- Select the default Link Qualifier.
- Then click on “Submit”.
- Finally click on “Save”. There are no changes to reconcile.



Username: superman
First Name: Clark
Last Name: Kent
Email Address: clark.kent@iamsuperman.com

Fig 7. Creating new users in OpenIDM

The fig 7 elaborates about how the users can be created in OpenIDM.



Source object has no matching target.

Assign a default action, workflow or script.

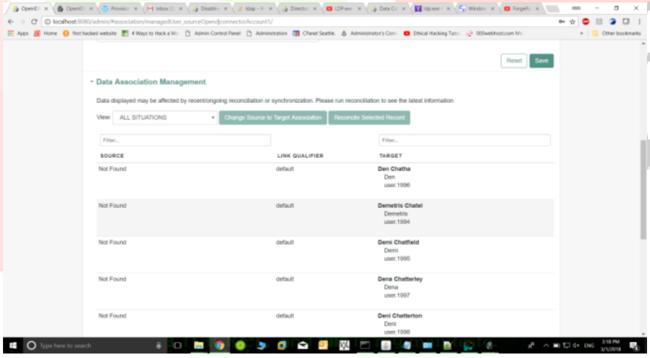
Create ★

Creates a new record in the target system.

★ Default ☆ Valid action

Fig 8.Policy Actions in OpenIDM

In Fig 8. elaborates the policy actions that needs to be taken care in OpenIDM


localhost:8080/admin/#association/managedUser_sourceOpendjconnectorAccount1/
Reset
Save
Data Association Management
View:
Change Source to Target Association
Reconcile Selected Record
Filter...

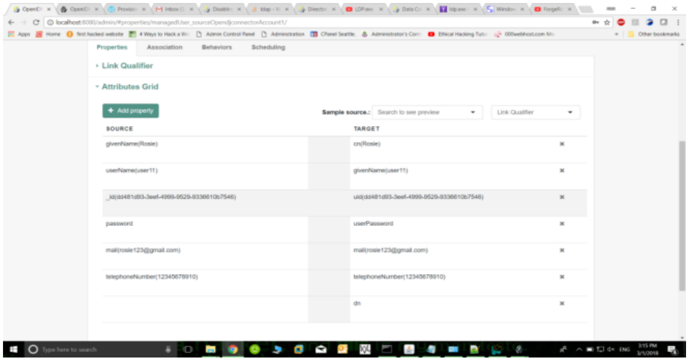
Data displayed may be affected by recent/ongoing reconciliation or synchronization. Please run reconciliation to see the latest information

View: ALL SITUATIONS

| SOURCE | LINK QUALIFIER | TARGET |
|---|---|---|
| Not Found | default | Den Chatha<br>Den<br>user.1996 |
| Not Found | default | Demetris Chatel<br>Demetris<br>user.1994 |
| Not Found | default | Demi Chatfield<br>Demi<br>user.1995 |
| Not Found | default | Dena Chatterley<br>Dena<br>user.1997 |
| Not Found | default | Deni Chatterton<br>Deni<br>user.1998 |

Fig 9. Data association management in OpenIDM

Data association is done between the source and target with a link qualifier

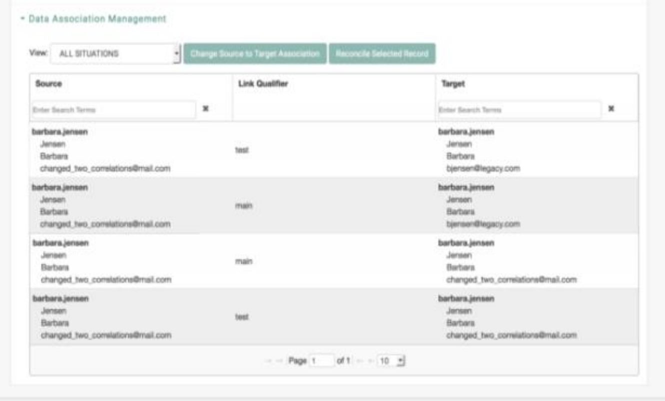


| SOURCE | TARGET |
|---|---|
| givenName(Rosie) | cn(Rosie) |
| userName(user11) | givenName(user11) |
| _id(dd481d93-3eef-4999-9529-9336610b7546) | uid(dd481d93-3eef-4999-9529-9336610b7546) |
| password | userPassword |
| mail(rosie123@gmail.com) | mail(rosie123@gmail.com) |
| telephoneNumber(12345678910) | telephoneNumber(12345678910) |
|  | dn |

Fig 10. Attribute fields of OpenIDM

Mapping of target fields in OpenIDM

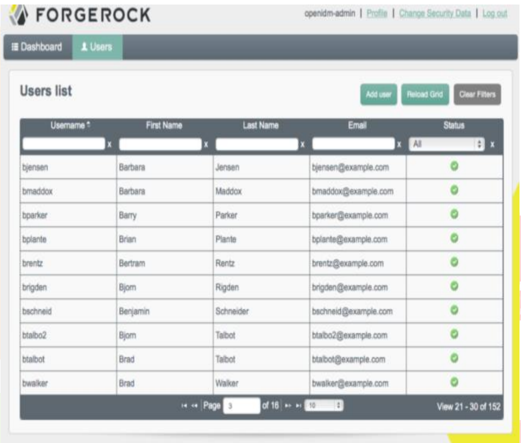
## VI. RESULTS AND ANALYSIS


Data Association Management
View: ALL SITUATIONS
Change Source to Target Association
Reconcile Selected Record
Enter Search Terms

| Source | Link Qualifier | Target |
|---|---|---|
| barbara.jensen<br>Jensen<br>Barbara<br>changed_two_correlations@mail.com | test | barbara.jensen<br>Jensen<br>Barbara<br>bjensen@legacy.com |
| barbara.jensen<br>Jensen<br>Barbara<br>changed_two_correlations@mail.com | main | barbara.jensen<br>Jensen<br>Barbara<br>bjensen@legacy.com |
| barbara.jensen<br>Jensen<br>Barbara<br>changed_two_correlations@mail.com | main | barbara.jensen<br>Jensen<br>Barbara<br>changed_two_correlations@mail.com |
| barbara.jensen<br>Jensen<br>Barbara<br>changed_two_correlations@mail.com | test | barbara.jensen<br>Jensen<br>Barbara<br>changed_two_correlations@mail.com |

Fig 11. Mapping of Source and Target users

In Fig 11. elaborates the mapping of source and target users with a link qualifier.

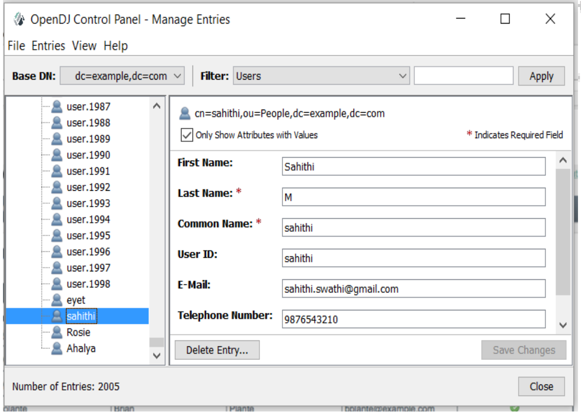


Users list

| Username | First Name | Last Name | Email | Status |
|---|---|---|---|---|
| bjensen | Barbara | Jensen | bjensen@example.com | ✓ |
| bmaddox | Barbara | Maddox | bmaddox@example.com | ✓ |
| bparker | Barry | Parker | bparker@example.com | ✓ |
| bplante | Brian | Plante | bplante@example.com | ✓ |
| brentz | Bertram | Rentz | brentz@example.com | ✓ |
| brigden | Bjorn | Rigden | brigden@example.com | ✓ |
| bschneid | Benjamin | Schneider | bschneid@example.com | ✓ |
| btalbo2 | Bjorn | Talbot | btalbo2@example.com | ✓ |
| btalbot | Brad | Talbot | btalbot@example.com | ✓ |
| bwalker | Brad | Walker | bwalker@example.com | ✓ |

Fig 12. Users list in OpenIDM

In Fig 12. Elaborated the list of user in OpenIDM after integrating the components of Forgerock



Base DN: dc=example,dc=com

Filter: Users

cn=sahithi,ou=People,dc=example,dc=com

☑ Only Show Attributes with Values

* Indicates Required Field

First Name: Sahithi

Last Name: * M

Common Name: * sahithi

User ID: sahithi

E-Mail: sahithi.swathi@gmail.com

Telephone Number: 9876543210

Number of Entries: 2005

Fig 13. OpenIDM users in OpenDJ

## VII. USE CASE DIAGRAM

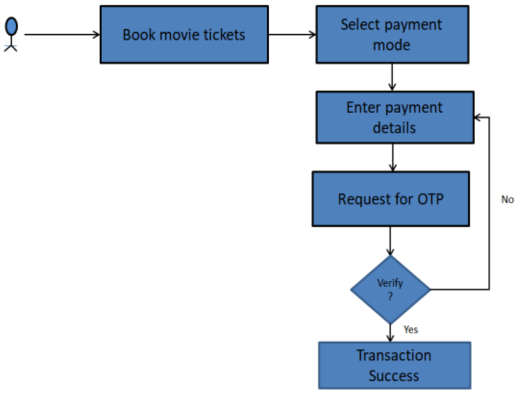


Fig 14. Transactional use case diagram

In the Fig 14 when the users wants to book a movie tickets, user has to select a payment mode in order to complete the transaction, then user enters the details and request for the OTP that request is generated by OpenAM and sent to users number for verification, if it is verified the user transaction is completed else user has to enter the details again.

## VII. CONCLUSION

This paper provides the overview of OpenIDM using Forgerock platform. OpenIDM helps to provide identity and access management to users. OpenIDM can be used to update the user's information automatically. OpenIDM also provide high security by using OpenIG.This proposed model works well in an environment where the data can be updated automatically and viewed by the authorized users. So, we may add additional algorithms to make it more secured and efficient.

## VIII. REFERENCES

[1].http://www.oracle.com/technetwork/middleware/id-mgmt/overview/oracle-idm-wp-11gr2-1708738.pdf

[2].https://www.giac.org/paper/gsec/3222/overview-secure-identity-management-idm/105201

[3].https://www.ibm.com/blogs/sweeden/getting-started-with-ibm-single-sign-on-for-bluemix/

[4].https://www.forgerock.com/resources/view/63280634/product-brief/identity-gateway-product-brief.pdf

[5].https://www.forgerock.com/app/uploads/2017/10/FR-WhitePaper_IdentityManagement-Letter.pdf

[6].https://www.paradigmo.com/images/downloads/RockKit-WhitePaper.pdf

[7].https://backstage.forgerock.com/docs/opendj/2.6/OpenDJ-2.6-Admin-Guide.pdf

[8].https://www.forgerock.com/platform/access-management

[9].https://www.forgerock.com/resources/view/64984501/product-overview/forgerock-access-management.pdf

[10].https://www.cloudshare.com/blog/training/forgerock-success-story-boost-software-training-lms-virtual-labs-integration