**IDENTITY MANAGEMENT THROUGH SAILPOINT**

A PROJECT REPORT

*Submitted by*

**Sayan Mandal**(15BCE1344)

*in the partial fulfillment for the award*

of

# Bachelor of Technology

in

# Computer Science and Engineering



**Vandalur - Kelambakkam Road, Chennai - 600127**

**July - 2019**



## School of Computing Science and Engineering

### DECLARATION

I hereby declare that the project entitled “Identity Management through Sailpoint” submitted by to the School of Computing Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai 600127 in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a record of bonafied work carried out by us under the supervision of Prof. Viswanathan V. I further declare that the work reported in this project has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma of this institute or of any other institute or university.

Place: Chennai Signature of Candidate (s)

Date:

Sayan Mandal (15BCE1344)

#### II



**School of Computing Science and Engineering**

### CERTIFICATE

This is to certify that the report entitled “Identity Management through Sailpoint” is prepared and submitted by Sayan Mandal (15BCE1344) to VIT Chennai, in partial fulfillment of the requirement for the award of the degree of B. Tech CSE program is a bonafide record carried out under my guidance. The project fulfills the requirements as per the regulations of this University and in my opinion meets the necessary standards for submission. The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma and the same is certified.

|  |  |  |
| --- | --- | --- |
| Guide | Program Chair | |
| Name: Dr. Viswanathan V | Name: Dr. Justus S | |
|  |  |
| Date: | Date: |  |
|  |  |  |
| External Examiner  Signature:  Name:  Date: | Internal Examiner  Signature:  Name:  Date:  **III** | Internal Examiner  Signature:  Name:  Date: |

### ACKNOWLEDGEMENT

I wish to express our sincere thanks to a number of people without whom I could not have completed the project successfully.

I would like to place on record our deep sense of gratitude and thanks to my external guide **Mr. Hironmoy Dasgupta**, Sr. Architect - Technology, Cognizant Security - IAM, KOL - GTP, Cognizant Technology Solutions and **Mrs. Santhi Kaza**, Delivery Partner, Cog Sec – Core, BLR – MBP, Cognizant Technology Solutions whose esteemed support and immense guidance encouraged us to complete the project successfully.

### I would like to thank our Program Chair Dr. Justus S & Co-Chair, Dr. C

**Sweetlin Hemalatha**, B.Tech. Computer Science and Engineering and **Project Coordinator** **Dr. B.V.A.N S.S. Prabhakar Rao,** VIT Chennai campus, for their valuable support and encouragement to take up and complete the thesis.

### Special mention to my senior employees Vivek Kumar Mohanty, Amit Kumar Dey, Sreetama Gayen and Diksha Kesari for spending their valuable time and efforts in sharing their knowledge and for helping us in every minute aspect in the project. I also want to sincerely give my gratitude to my project mates – Anmol Singh and Kumar Aniket for their efforts to complete the project with me.

We thank the management of Cognizant Technology Solutions for permitting me to use the library and online resources. I also thank all the respected senior members for giving us the basic knowledge about security and courage and the strength that I needed to complete my goal. This acknowledgment would be incomplete without expressing the whole hearted thanks to my family and friends who motivated me during the course of our work.

Sayan Mandal (15BCE1344)

**IV**

### Table of Contents

### 

#### List of Figures

### List of Abbreviations

### EXECUTIVE SUMMARY

Through this project, I am able to learn and expertise in the software called “SailPoint IdentityIQ”. With this software, we can provide Identity and Access Management facilities to any organization or their clients. SailPoint's identity governance solutions provide complete visibility into who is doing what, what kind of risk that represents and allows you to take action. It links users, applications, data and devices to create an identity enabled enterprise. This project is divided into different modules like setting up the environment, deploying SailPoint, on boarding the application, creating the entire identity cube from different data sources. The project includes performing various tasks such as identity mapping, data aggregation, assign roles, entitlement creation, provisioning and de-provisioning, creating forms and Quicklinks which are used to update the access, performing a manager approval scheme that sends a request to the manager for access required by the user. The manager decides the approval or rejection of the request. This project is based on the knowledge gained on SailPoint, all its functionalities and modifications made in this software according to our own requirements. This project mainly focuses on identity administration and access governance system. The principle feature of this project is its ability to support group and role-based access management. Lastly through Plugins managing workitems has been version independent.

### ABSTRACT

Everybody in this world is different from one another and how much one is unique from others is determined by his identity, which differ for everyone. We can identify someone by his name, gender or appearance or some unique characteristic features but a system cannot identify someone based on these traits. Now using these traits and combined them one unique identity can be created for an individual which will help the system that it is the right individual. The project aims to create identities for individuals which will have some basic information about the individuals. As **“Sailpoint”** is new to the market and dominating with its fast, flexible features it is used as the base identity management software for the project. Also, through this software any rights, capabilities or roles of a particular individual in an organization can also be determined. This project aims to create identity from a trustworthy source file and then manage those created identities, like- assign roles, giving entitlements or any kind of updation (changes) in those identities and all these tasks are handled through the software, “Sailpoint”.

### INTRODUCTION

Before entering to the project details there are some related topics which need to be discussed. Identity in an organization is created not only to identify an individual but also to restrict his movements or observe what he is doing, i.e. to maintain a secure environment to prevent anyone from exposing necessary information from the unwanted ones. So, to prevent these kind of information which is shared across the world through internet a subject/branch **“Cyber Security”** has been developed throughout the years.

In this organization the security is divided in four basic towers, like-

1. IAM
2. IVM
3. ITM
4. GRC

These towers work side by side to maintain the integrity of the company.

* 1. **Objective**

The objective of this project is to learn and expertise in the software called “SailPoint IdentityIQ”. This software is used to provide Identity and Access Management facilities to any organization or their clients. The implementation of this project will provide a complete identity and access management control to any business. By solutions of this software we can assure that right people have right access at right time and it provides complete visibility into who is doing what, what kind of risks are present and accordingly allows us to take the action. By using this software, we can link people, applications, data and devices to create an identity-enabled enterprise. The benefits of this project are automated provisioning and access control to applications and data. The efforts, errors and time are reduced across access requests. We have an accurate access reporting of who has access to what and if the access is appropriate or not.

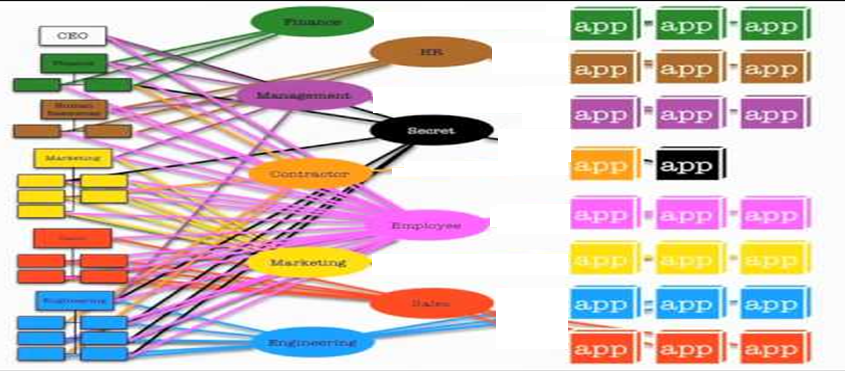
Hence, the main objective is to develop expertise in this software by learning it from scratch that how it works, what are its applications, limitations and how to implement any real-time or client projects using this software for any business or enterprise.

* 1. **Background**

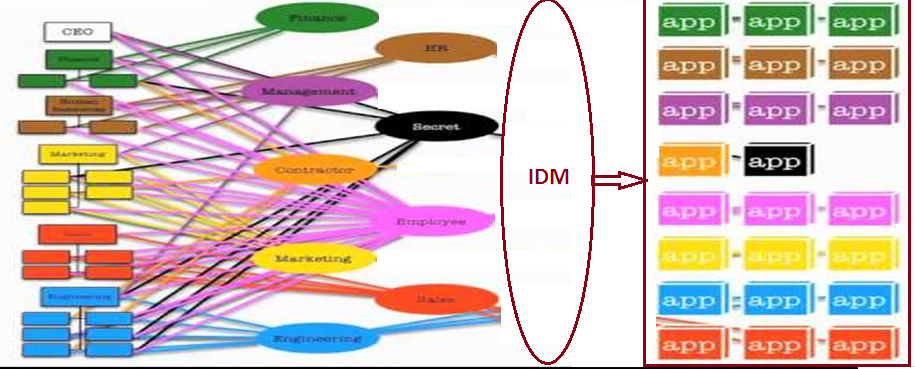
SailPoint was founded in 2005 by Mark McClain and his co-founders. They promised to provide innovative solutions to business problems and an exciting, collaborative work environment for identity rock stars. Together, they redefined identity’s place in the security ecosystem. SailPoint Technologies, Inc. designs, develops, and markets identity governance software that helps organizations govern user access to critical systems and data. It offers Identity Alliance that allows companies to integrate disparate security and infrastructure components, IdentityNow (a SaaS identity governance solution for enterprises), IdentityIQ (an enterprise solution that enables the client to gain visibility and manage access to various resources) and Identify IQ File Access Manager (to identify governance for files for unstructured data). The pre-requisite required for using this software is the knowledge JAVA programming language, handling of database etc.

* 1. **Motivation**

As the fastest-growing, independent Identity and Access Management (IAM) provider, SailPoint help hundreds of the world’s largest organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices, and in the cloud. SailPoint provides the organizations an integrated set of core services including identity governance, provisioning, and access management delivered on-premises or from the cloud (IAM-as-a-service). The motivation for learning this software is surely, because it is competing and winning against some very large companies in the identity management market because of the innovative products created through SailPoint. It is a new software in the market and very less people are there who gets an opportunity to work on this software. As this software is trending in the identity and access management solution for businesses of all sizes, hence gaining knowledge about this software and learning it gives us a very good opportunity to get an upper hand on this software and build our career in this domain. It offers innovative identity and access management resolutions for administration, provisioning, and access management on-premises or IDaaS



Before IDM integration in an organization



After IDM integration in an organization

### PROJECT DESCRIPTION AND GOALS

#### Project Description

The implementation of this project will provide a complete identity and access management control. Our project includes implementing the modules and tasks assigned by our mentor and learn the steps and process about the working of SailPoint. These tasks are described as follows:

* Set up environment.
* Deploy SailPoint IIQ on local host.
* Application Onboarding
* Import Data from CSV file and MySQL database.
* Creating identity cube from Different Data Source.
* Data Aggregation.
* Identity Mapping.
* Role and Entitlement Creation
* Modify existing user access
* Setting approval Schemes
* Providing Birthright access to new Joiners
* User Provisioning to On-Premises System (MySQL)
* User De-provisioning to On-Premises System
* QuickLinks and Forms.
* Update Access (Entitlement) using Forms.
* Update Access (Entitlement) with Manager Approval module.
* Creating a custom Plugin and its deployment.

* 1. **Goals**

The main goal of learning SailPoint is to help the organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices, and in the cloud. By learning this software, we can easily set up the environment for using SailPoint, we can easily create identities, we can easily aggregate the data, perform Provisioning and De-provisioning, update access using QuickLinks and Forms, performing a manager approval scheme. Lastly, through Plugins provide user with a flexible environment which they can import, do the work and after that when the work is completed they can delete the plugin which will not affect the IIQ application.

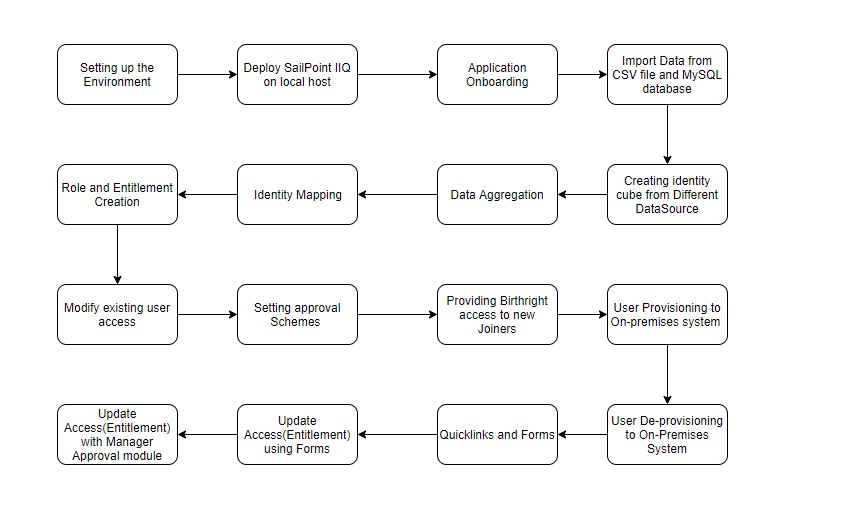
1. **TECHNICAL SPECIFICATION**
   1. **Software Specification**

The tools and software’s used for this project are described as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Sl. No. | Software | Version | Description |
| 1. | Sailpoint IdentityIQ | 7.2 | It is a software used to provide Identity and Access Management facilities to any organization or their clients. It is a premiere identity management software that provides complete identity and access management control to any business. It provides complete visibility into who is doing what, what kind of risk are present, and allows you to take action. It links people, applications, data and devices to create an identity-enabled enterprise. |
| 2. | Apache Tomcat | 8.5.5 | It is an open source implementation of the Java Servlet, JavaServer Pages, Java Expression Language and Java WebSocket technologies. The Java Servlet, JavaServer Pages, Java Expression Language and Java WebSocket specifications are developed under the Java Community Process. This software powers numerous large-scale, mission-critical web applications across a diverse range of industries and organizations. |
| 3. | MySQL | 5.7 | MySQL is a freely available open source Relational Database Management System (RDBMS) that uses Structured Query Language (SQL). SQL is the most popular language for adding, accessing and managing content in a database. It is famous for its quick processing, proven reliability, ease and flexibility of use. |
| 4. | Eclipse Mars | 4.5.2 | Eclipse is an integrated development environment (IDE) used in computer programming, and is the most widely used Java IDE. It contains a base workspace and an extensible plug-in system for customizing the environment. |
| 5. | OpenDJ | 2.6.4 | It is a directory server which implements a wide range of Lightweight Directory Access Protocol (LDAP) and related standards, including full compliance with LDAPv3 but also support for Directory Service Markup Language. It also offers multi-master replication, access control, and many extensions. |
| 6. | Notepad++ | 7.5.9 | Notepad++ is a free source code editor and supports several languages (i.e. java, C++, SQL etc.). It uses pure Win32 API and STL which ensures a higher execution speed and smaller program size. |
| 7. | JD-GUI | 0.3.3 | It’s a java decompiler which decompile an Executable Java File (.jar) and open the java project with its classes and packages. |

### DESIGN PLAN

##### Design Approach



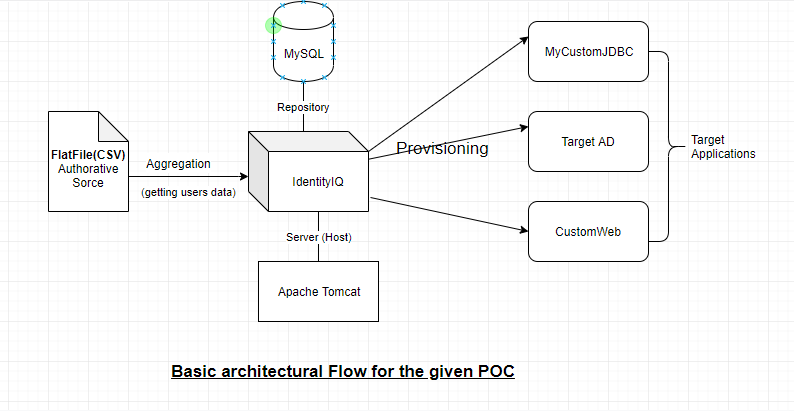
#### Figure 17: Flow Diagram

The Software Development Life Cycle process that we used was the Agile process. The reason for choosing Agile process is that we constantly wanted to update our work process and make the best design based on the reviews given by the doctors, our guide and the panel members. While the general idea and the problem statement was defined, we had to define more intricate details based on the feedback given by the doctors and mutual discussions with each other. The members working on the project were dedicated and ready to work despite the time and distance constraints.

Benefits of using the Agile process for our project:

1. We could incorporate all the suggestions given by the doctors, our guide and panel members.
2. We could make major design changes according to the suggestion of the subject matter experts.
3. We could complete the project on time and achieve the stretch goals of our project.
4. We could integrate the different modules developed under a single umbrella providing a comprehensive and scalable solution.
5. The rapid development of prototypes for testing purpose could be completed within the timelines and could be tested and verified.
6. The flexibility provided to work.

##### Use Case Diagram



#### Figure 18: Use Case Diagram

### PROJECT MODULES

The project is divided into four modules each of which consists different components and has different working principles which are describe in details below:

* 1. **Identity Creation:**

Firstly, from a trusted source (authoritative source) all the data are aggregated into IIQ through an application and using ***“Identity Mappings”*** which map the attribute of the data file with the IIQ attributes and this way the identities are created.

* 1. **Provisioning:**

This module mainly focuses on the user rights. In this module which identity should have which application, which entitlements, which roles etc. is decided. Also if any identity has to be modified and who will make the last decision on that change so that it will reflect on that particular identity is also dealt in this module.

* 1. **QuickLinks:**

How one QuickLink can be created and what functionality should the QuickLink will deliver to the user is discussed in this module.

* 1. **Plugin:**

Basically a plugin

### CODES AND STANDARDS

### 

The codes of this project cannot be shared because of the confidential data, according to the company’s rules and policies.

### CONSTRAINTS AND ALTERNATIVES

The only constraint in this project is that I have used local host to deploy this application rather than a web server. Mostly, all the features of SailPoint are working on local host but to get a fully functional service that can be used by the organization, for that we have to deploy the software on a web server which will cost some amount. This is the only constraint in this project that I used local host instead of a web server.

There are few alternatives for this software such as:

* **Okta**

Okta is a publicly traded identity and access management company, which provides cloud software that helps companies, manage and secure user authentication into modern applications, and for developers to build identity controls into applications, website web services and into devices.

* **CyberArk**

CyberArk is a publicly traded information security company offering Privileged Account Security. The company's technology is utilized primarily in the financial services, energy, retail, healthcare and government markets.

**33**

### SCHEDULES, TASKS AND MILESTONES

#### Timeline

|  |  |
| --- | --- |
| Task 1 | Setting up environment |
| Task 2 | Deploy SailPoint IIQ on local host |
| Task 3 | Application Onboarding |
| Task 4 | Import Data from CSV file and MySQL database |
| Task 5 | Creating identity cube from Different Data Source |
| Task 6 | Data Aggregation |
| Task 7 | Identity Mapping |
| Task 8 | Role and Entitlement Creation |
| Task 9 | Modify existing user access |
| Task 10 | Setting approval Schemes |
| Task 11 | Providing Birthright access to new Joiners |
| Task 12 | User Provisioning to On-premises system |
| Task 13 | User De-provisioning to On-Premises system |
| Task 14 | QuickLinks and Forms |
| Task 15 | Update Access (Entitlement) using Forms |
| Task 16 | Update Access (Entitlement) with Manager Approval module |

#### Figure 21: Task Schedules

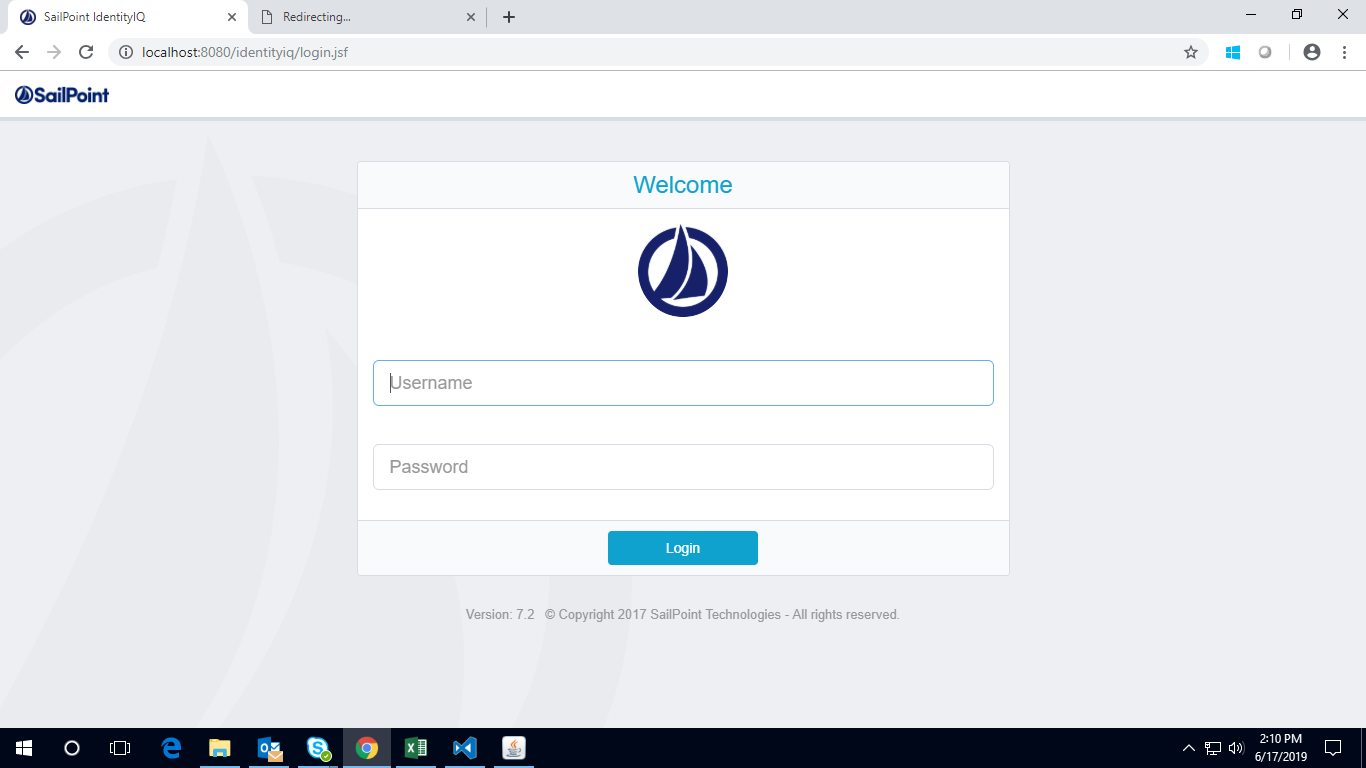
##### 9.2 Gantt Chart

Figure 22: Gantt Chart

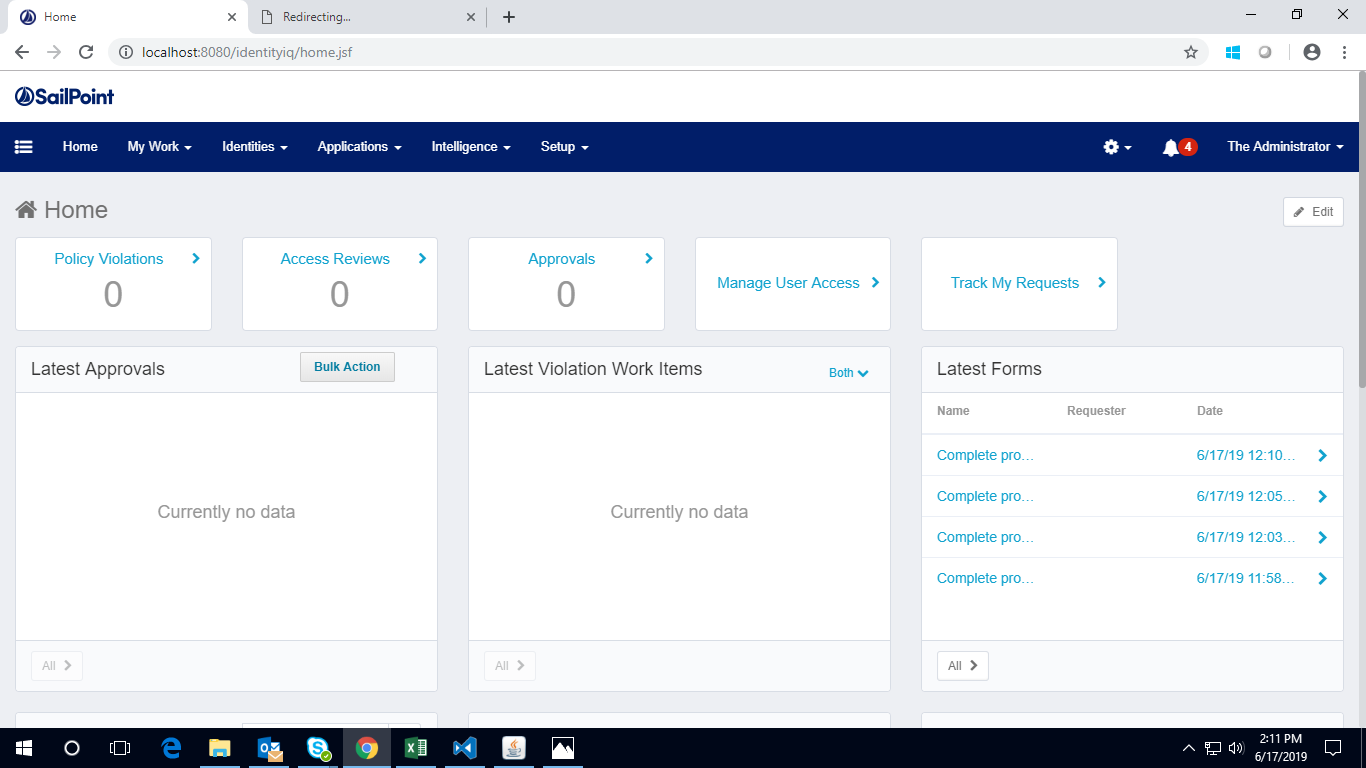
### PROJECT DEMONSTRATION

* 1. SailPoint installation

Firstly, .war file was moved to the Tomcat webapps folder. Then as soon as the server is started it automatically extracted the .war file into its directory. After the file has been extracted in the MySQL command line create\_identityiq\_tables-7.2.mysql file has been imported. Through this the database of SailPoint IIQ has been created. After that two files- a) init.xml and b) init-lcm.xml is imported in iiq console to initialize the configuration objects of SailPoint. Then, <http://localhost:8080/identityiq> url is entered for the login page which is shown in the figure------

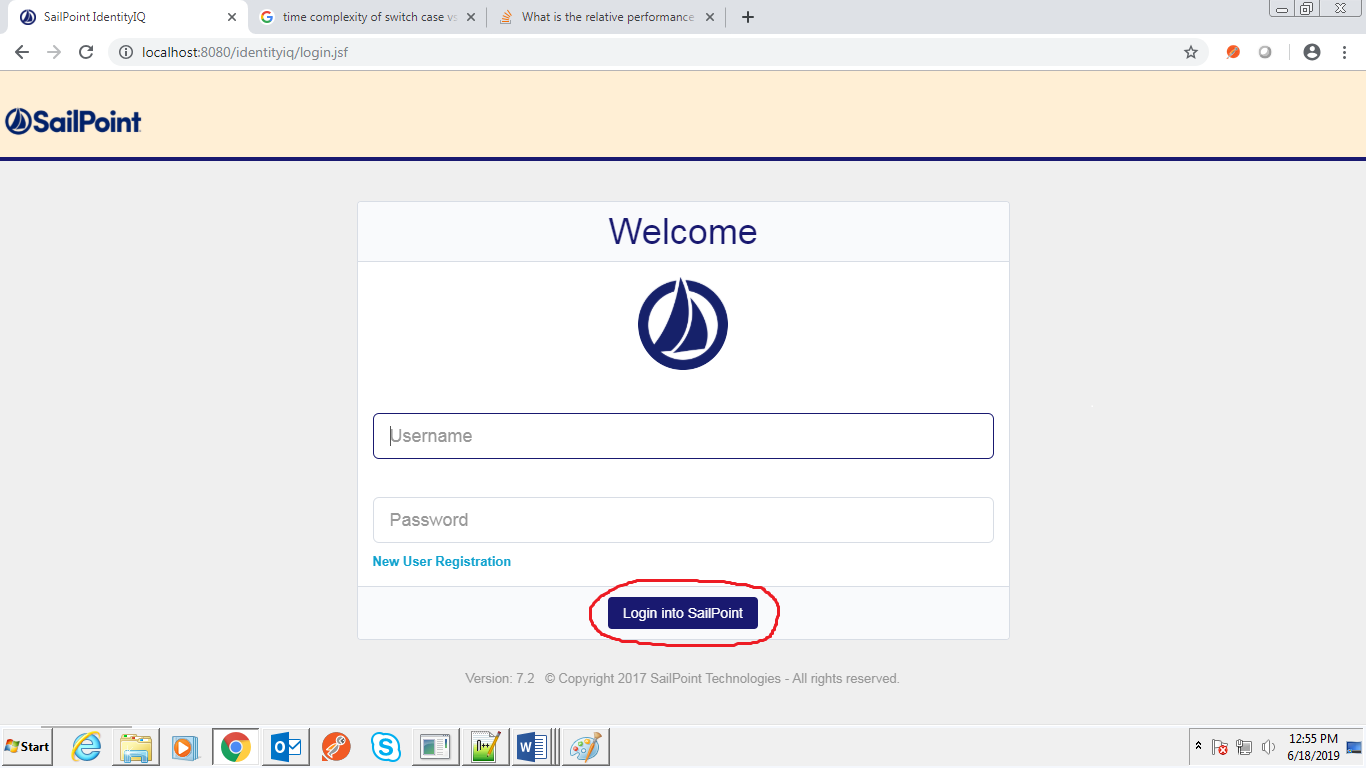


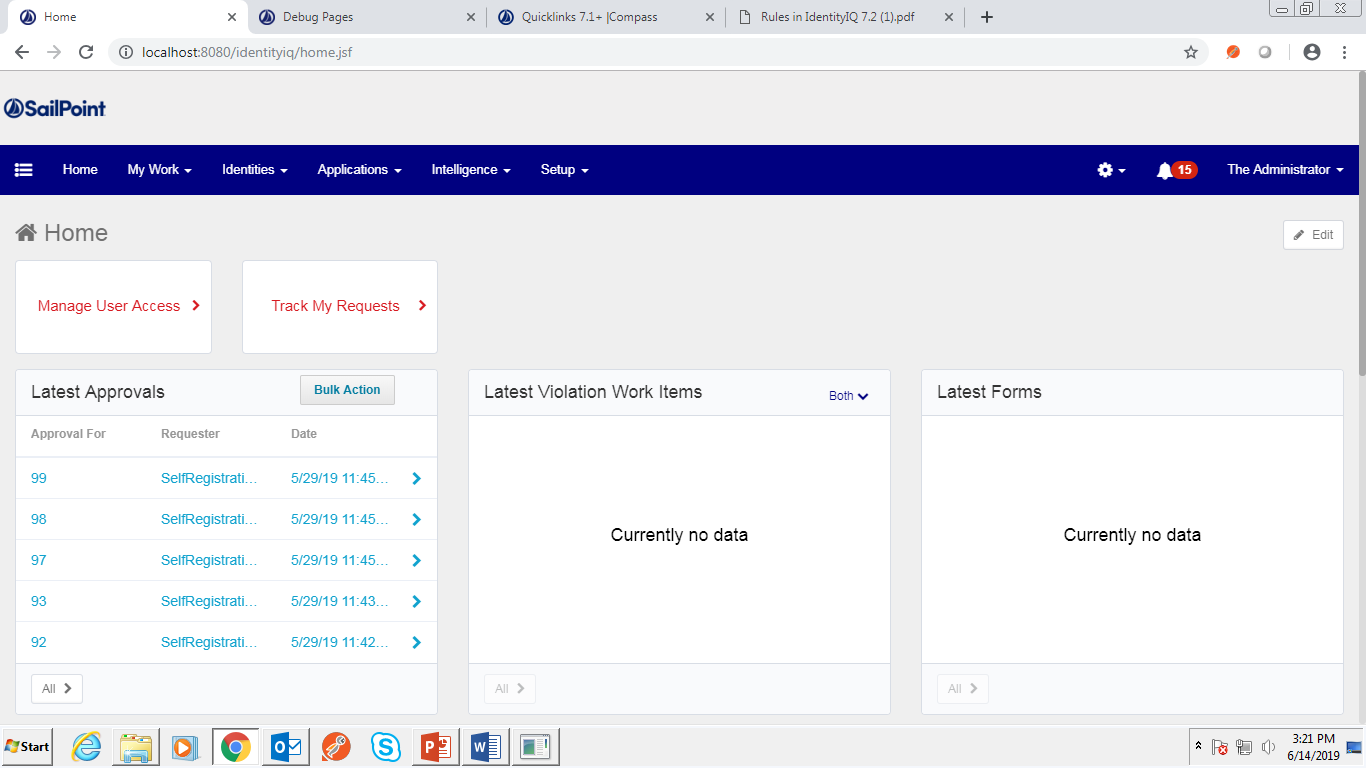
Providing the correct details user will be able to log in the application. In this case the default username which is spadmin and the default password which is admin, are entered to enter the application. The home page is shown in the figure……



* 1. Rebranding UI

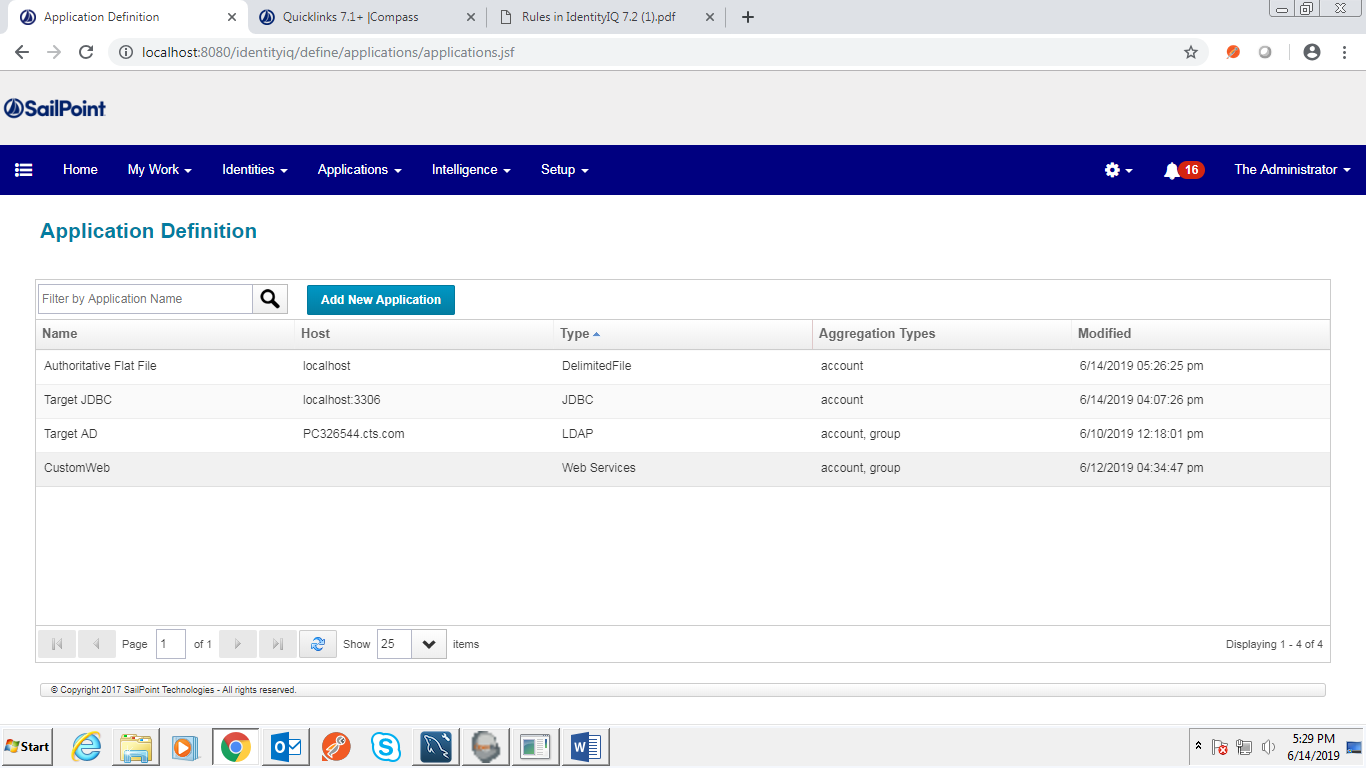
Here the basic UI (i.e. style, color, heading etc.) is changed from the default one.

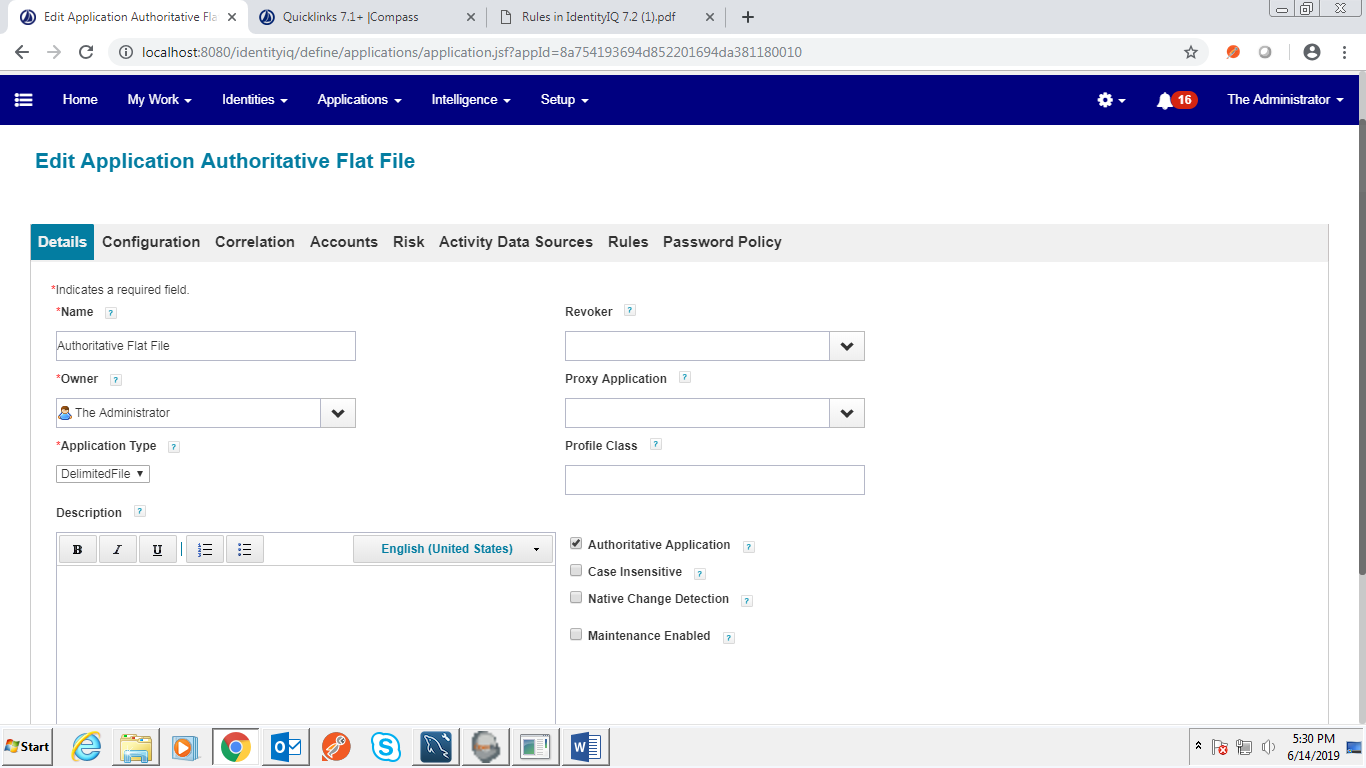




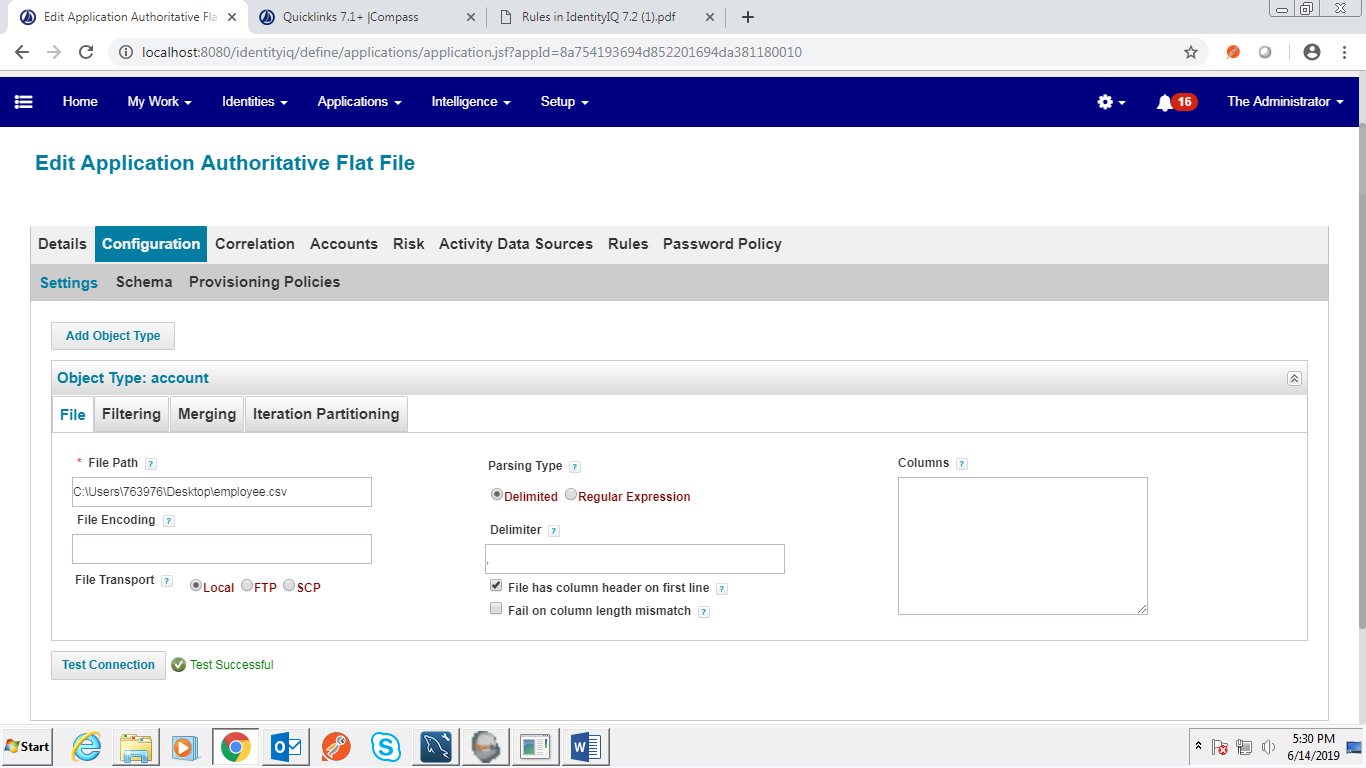
* 1. On-Premises Application Onboarding

After the complete deployment of SailPoint IIQ on localhost, three applications were created one as a source which is a CSV file (Authoritative Flat File) and another two as a target which are – a) through MySQL table (Target JDBC) and b) an active directory using LDAP (Target AD). Then the configuration of these applications was defined.



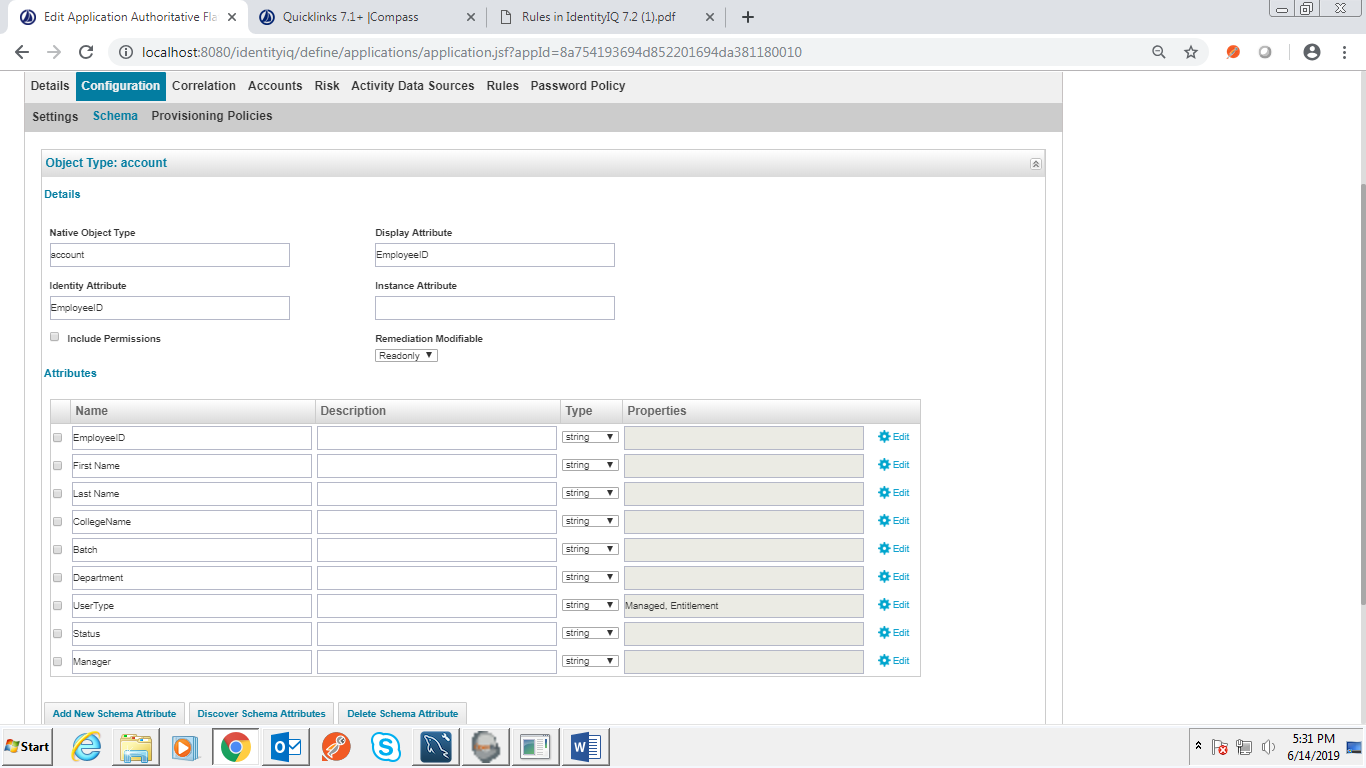


For Authoritative Flat File it was done by setting the path of the CSV file where it is located and also what token to be taken as delimiter when reading the file which has been shown in the Figure----. In this case “,” has been taken as a delimiter.



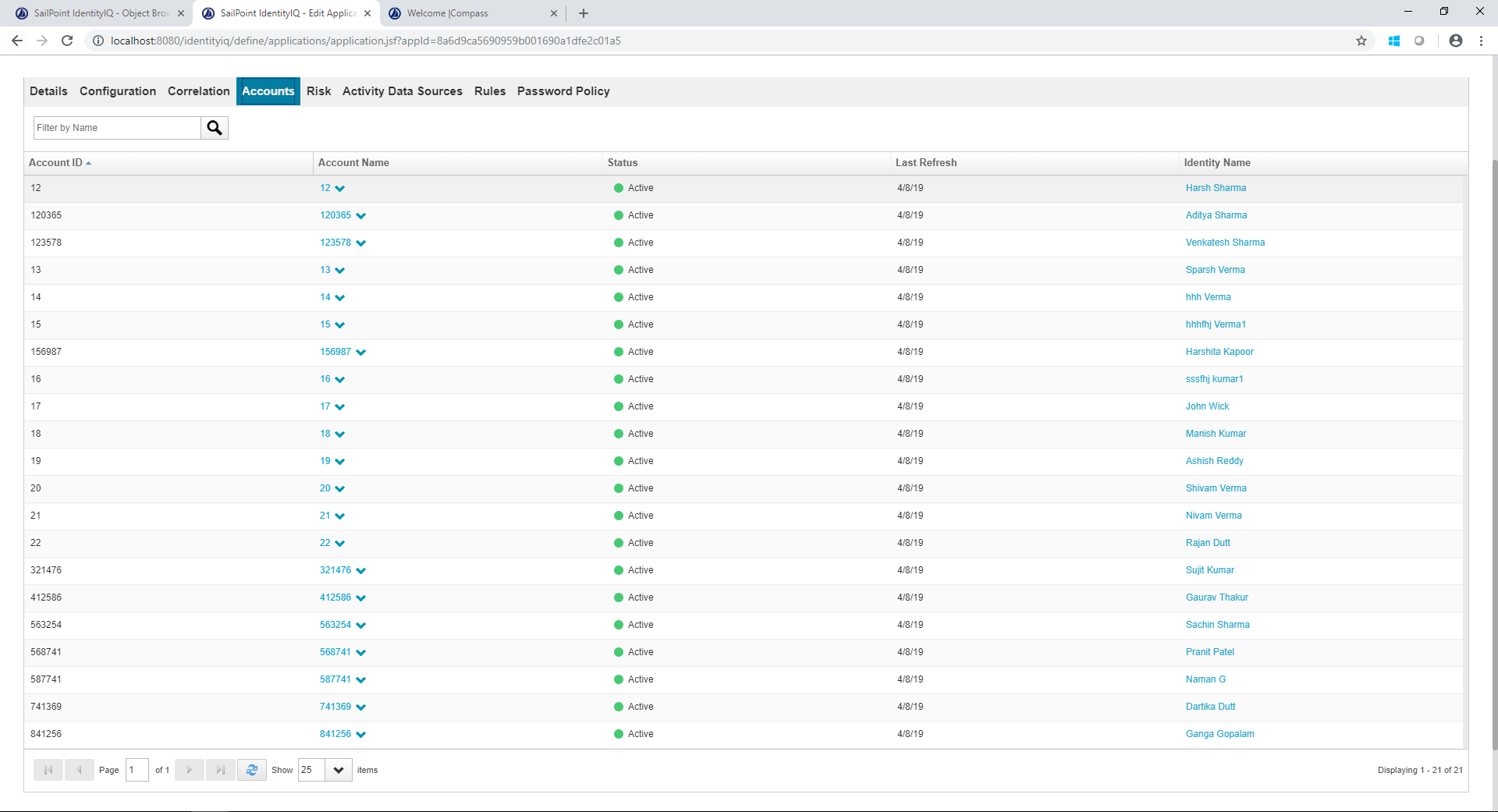
Whereas, Target JDBC and Target AD is used as our target system. For the first application the connection was made using JDBC connector by using the JDBC username, password and its URL and specifying the JDBC driver used and for the second application the connection was made using LDAP connector by using LDAP cn, ou, password, host name.

The attributes that were used in the CSV file are EmployeeID, First Name, Last Name, CollegeName, Batch, Department, UserType, Status and Manager which is shown in the figure---

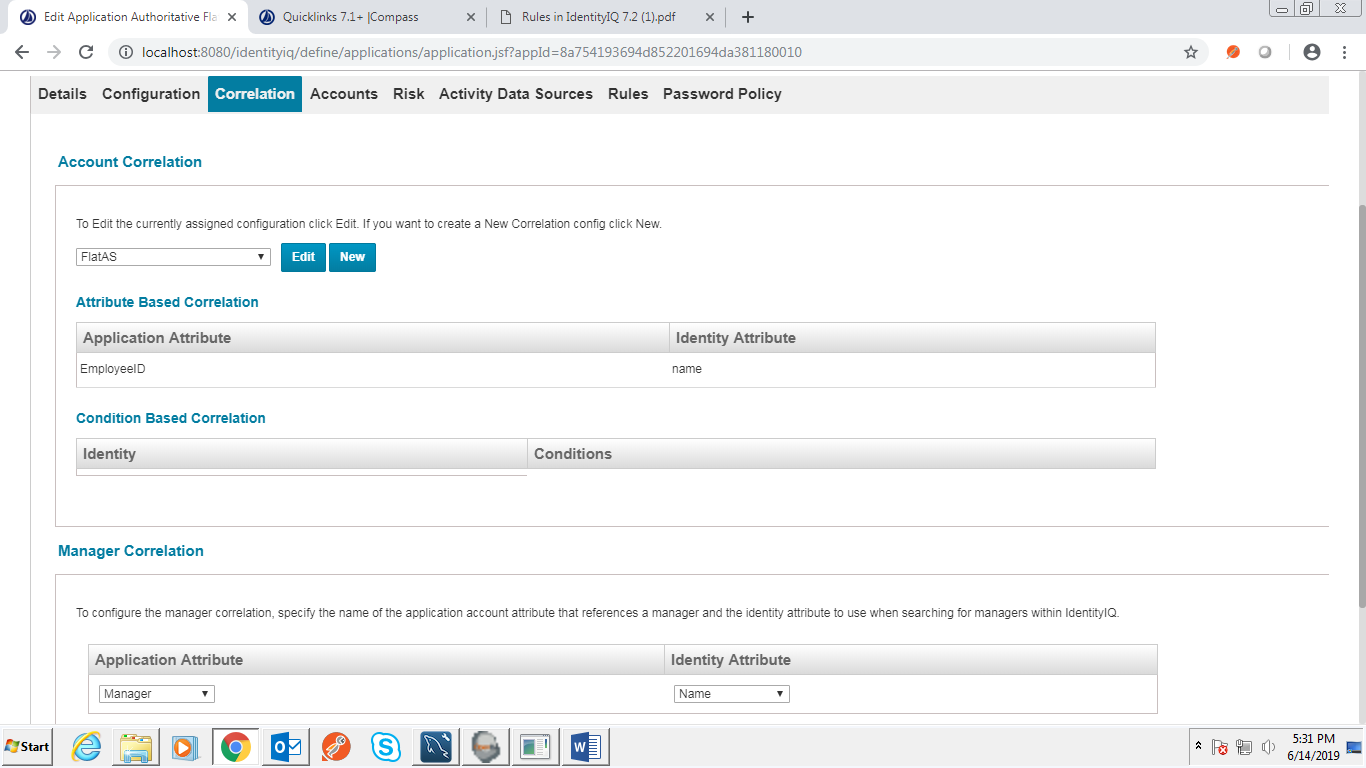


In Target JDBC there are two different tables **1)** app\_account **2)** app\_access.

In app\_access there are employee\_id, first\_name, last\_name, college, batch and status as attributes where employee\_id is the *PRIMARY KEY* of the table. The app\_access table contains two attributes i.e. employee\_id and entitlement where employee\_id is a *FOREIGN KEY* which is the reference of the *PRIMARY KEY* of app\_account. For the Target AD the attributes were Common Name, User ID, First Name, Last Name, Password, manager, initials. The identity attribute the applications was defined as ‘EmployeeID’, ‘employee\_id’ and ‘cn’. Identity Attribute is an attribute of an identity that provides identification of that identity. In figure 6.1.1, we can see the different accounts based on the id’s and their name which are displayed along with them.

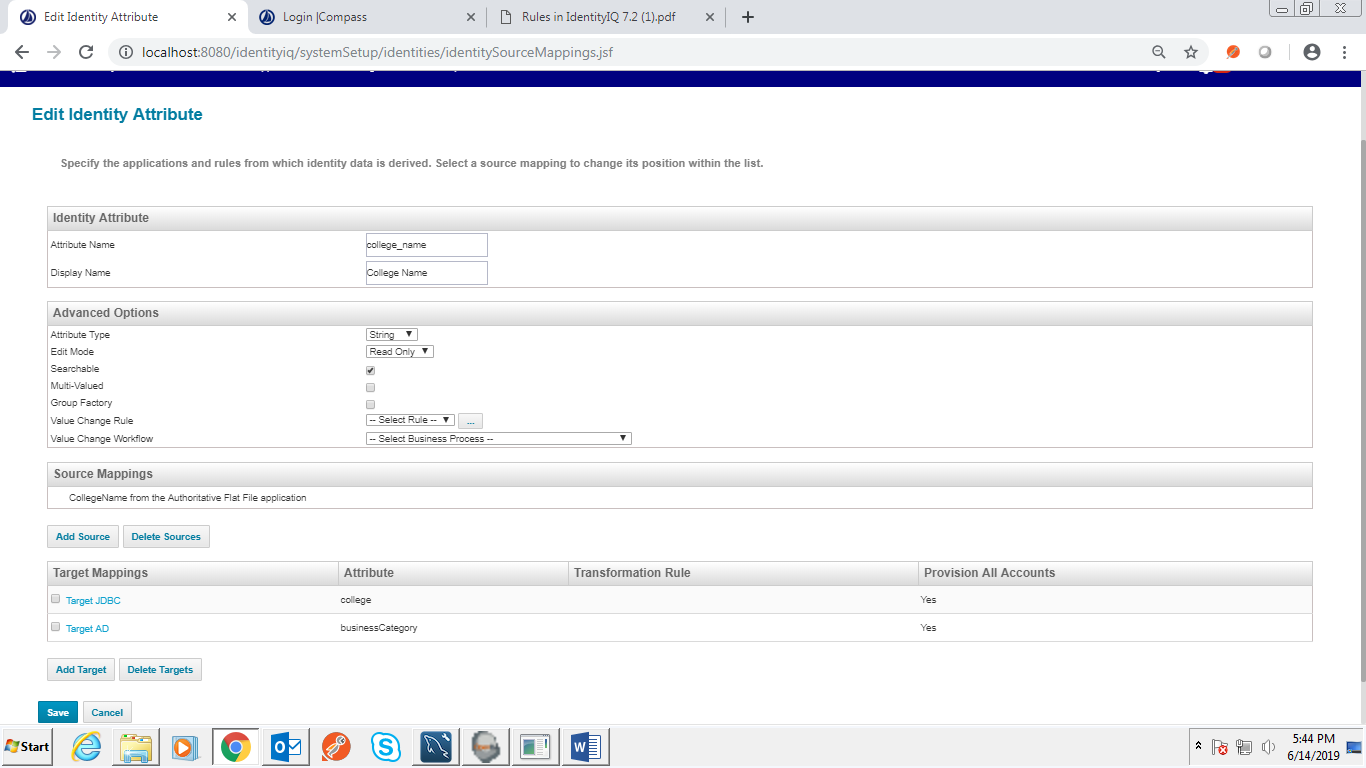
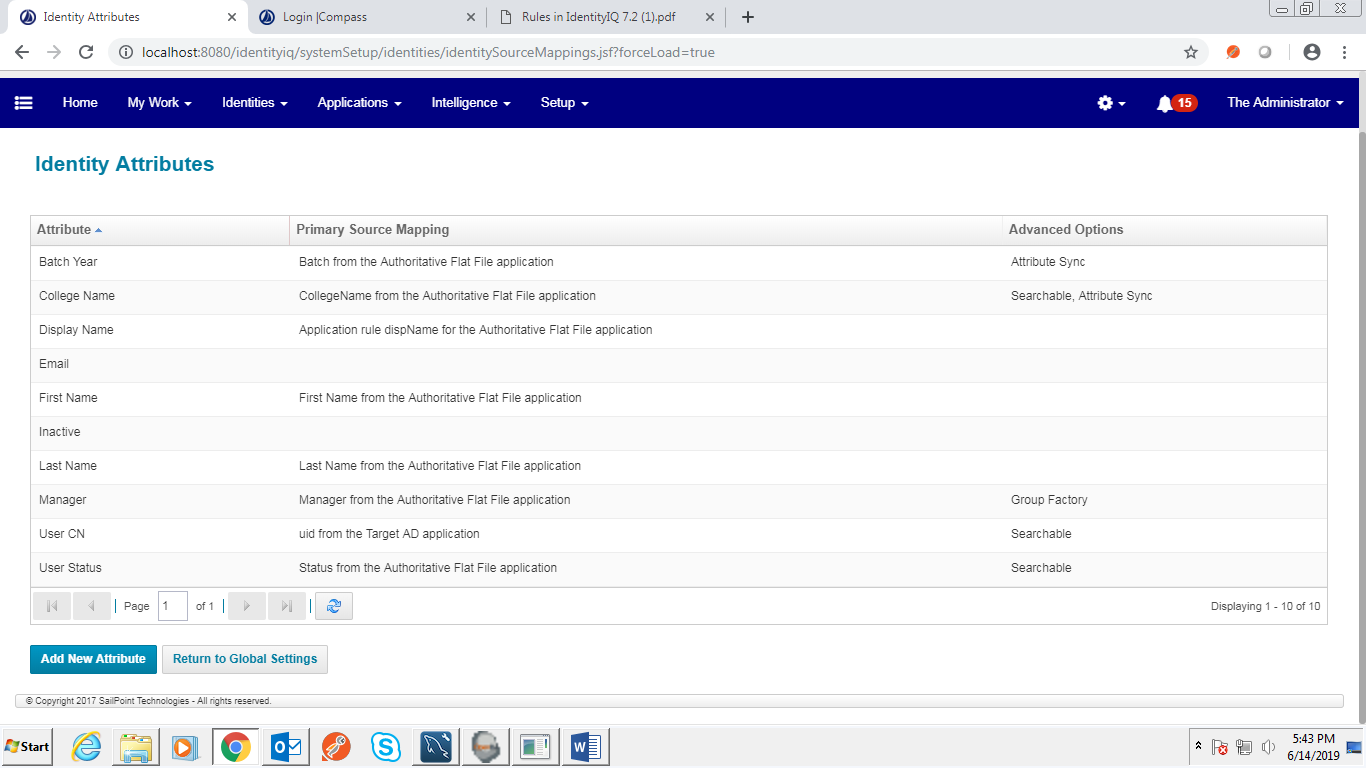


Then in figure --- correlation had been performed in which we have correlated the EmployeeID to the name attribute which is unique for IIQ application. In addition, for manger correlation, we used the manager id as an attribute and correlated it with the names of the other users.



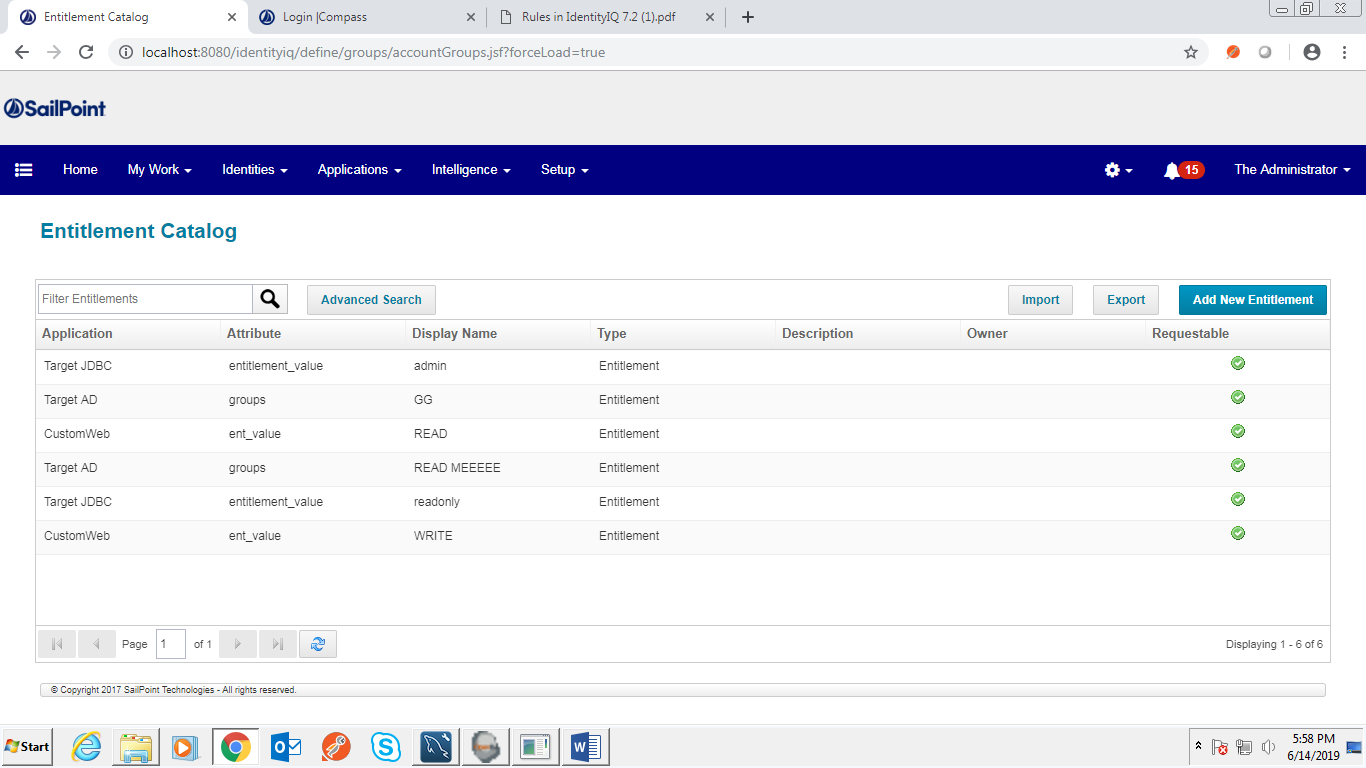
* 1. Defining extended Attributes for Identities

Identity mapping was performed which is used to configure the accounts that are managed by IdentityIQ. All the identities are mapped as per the requirement of the identity and were added through its source as shown in figures---



* 1. Role and Entitlement Configuration

Roles are defined based on the Target JDBC and Target AD application through which we have taken the name, owner and type of that application. In addition, the Entitlement is defined based on two categories for each application, for Target JDBC *readonly*, *admin* and for Target AD *GG*, *READ ME*. This changes from user to user based on the access given or provided to them. This access can be updated at SailPoint and in the target systems when required.

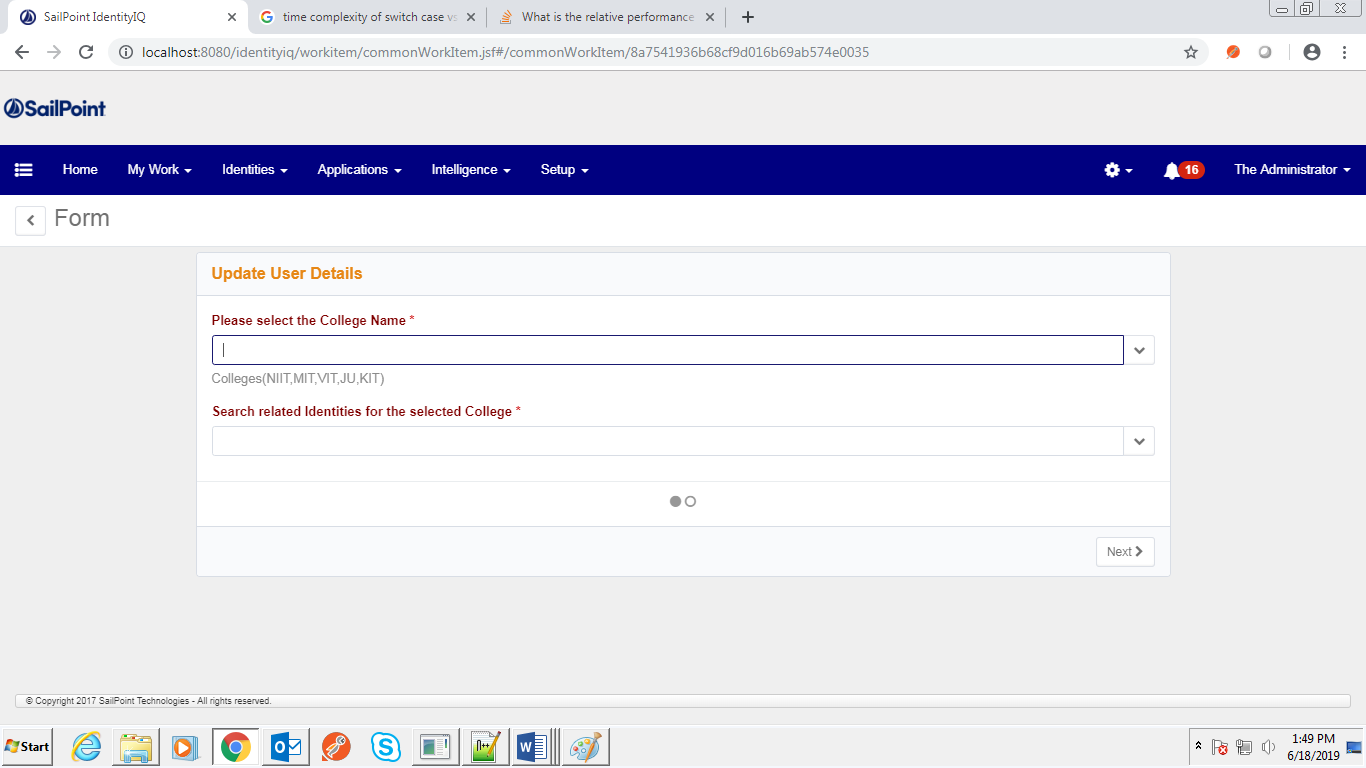


* 1. Providing Birthright Access through Roles

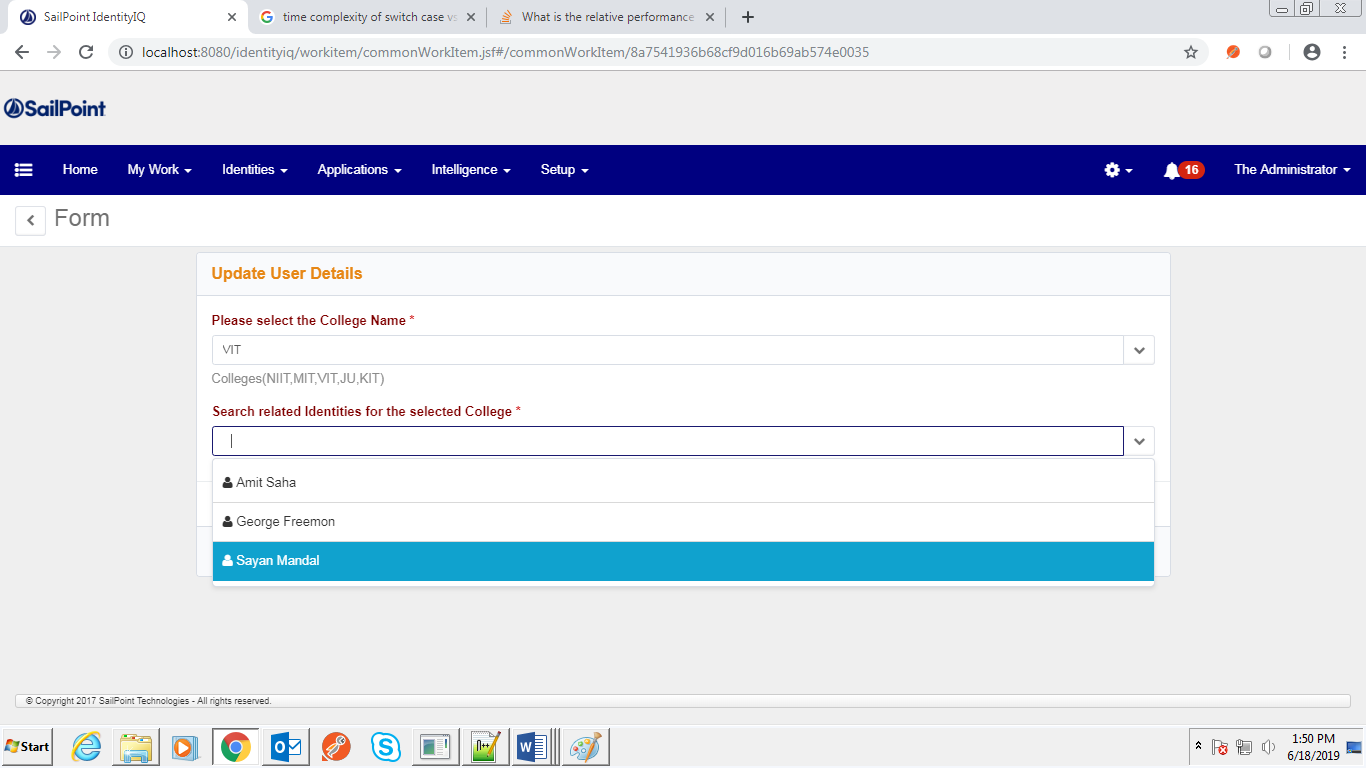
A *Business Role* was created which will be triggered when a new user joins and all the required access will be provided to him through this role. The role was created on the basis if the new user is active or not. If he is active then through this role birthright for the two target applications have been given to the user and he will be given access to these two applications. Below—

* 1. Providing form-based access Provisioning via QuickLink configuration

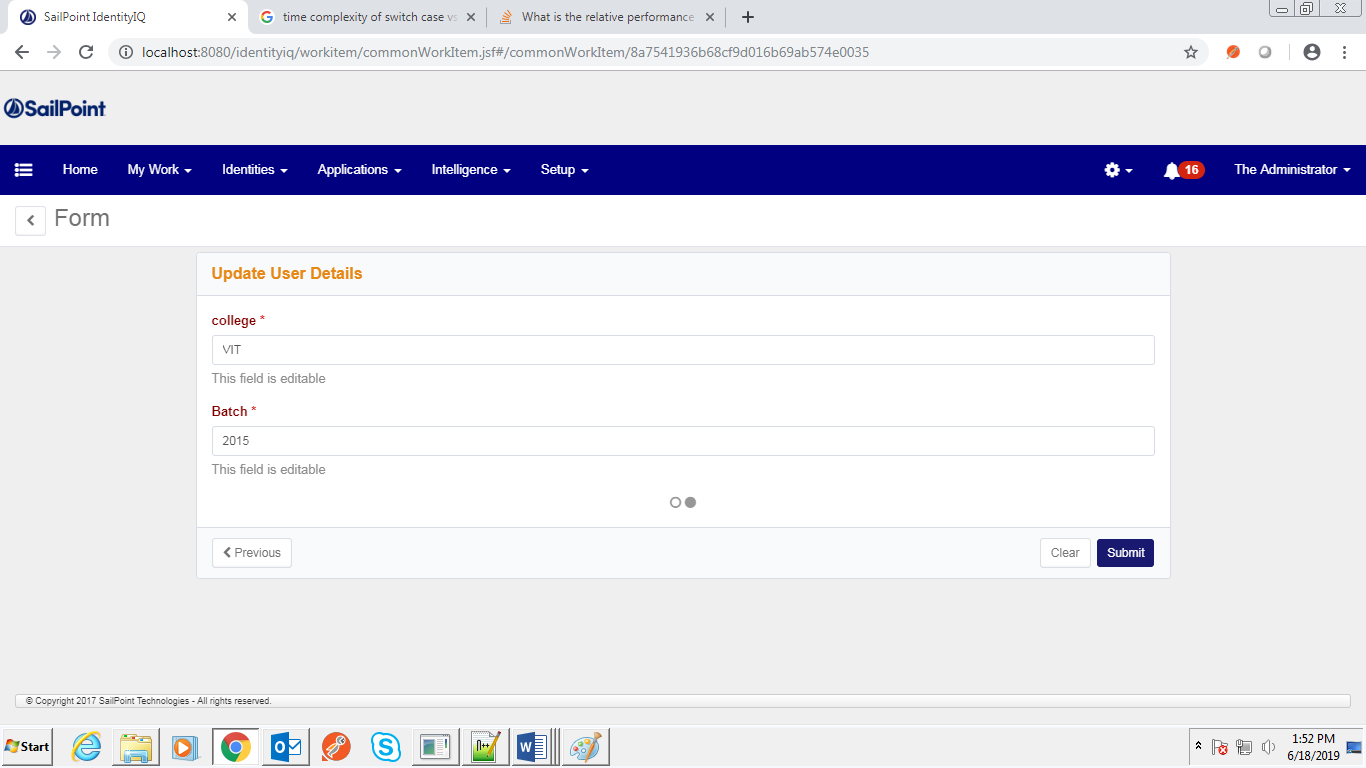
A workflow was created named Form Updation, which is used to update the college name and batch year in the target system and Sail Point. A user is able to update his/her access using this form as we can see in the figure 6.5.1.



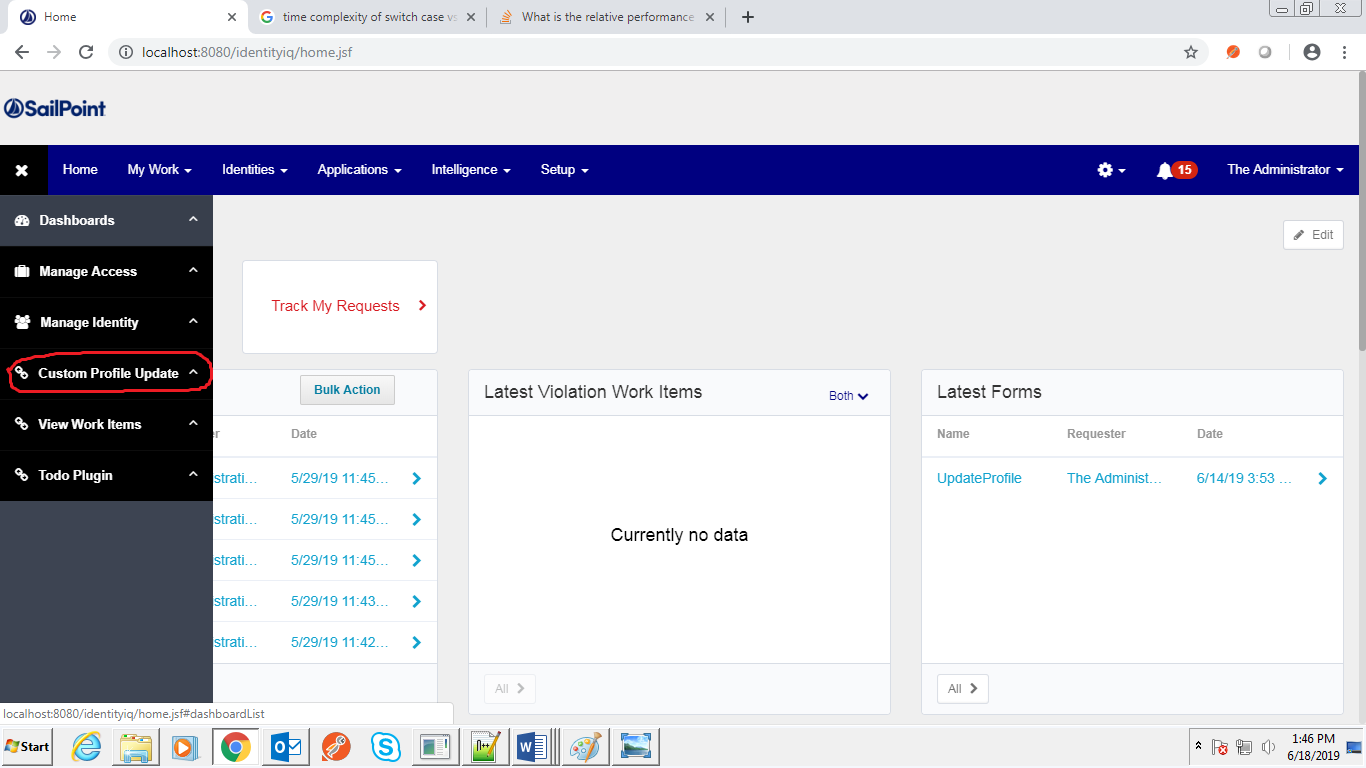
Whenever the user select a college all the identity which has the same college name will be shown in a dropdown manner as we can see in the figure---



After selecting the particular identity when they go to next page they can edit their previous information here and submit the form.



A QuickLink was created and on clicking on the QuickLink it takes the user to the form page (figure 6.5.2) which asks identity, target application, operation and Access that needs to be updated and if the manager module is not applied in workflow it approves the request for the identity selected in the form by the launcher of the event.

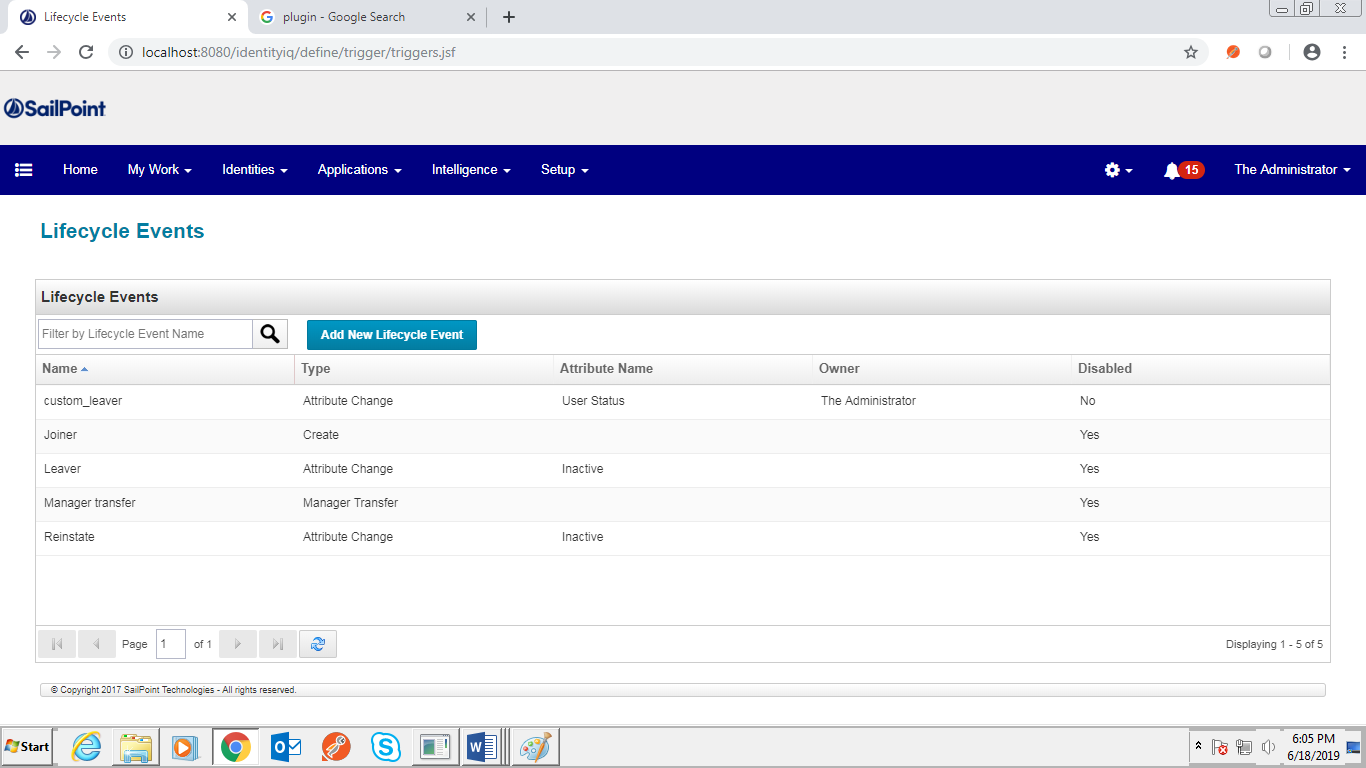


After submitting the form, it creates a work item for manager and sends the approval form to manager of the identity which upon clicking the approve button completes the task and updates the entitlement.

* 1. Lifecycle Events

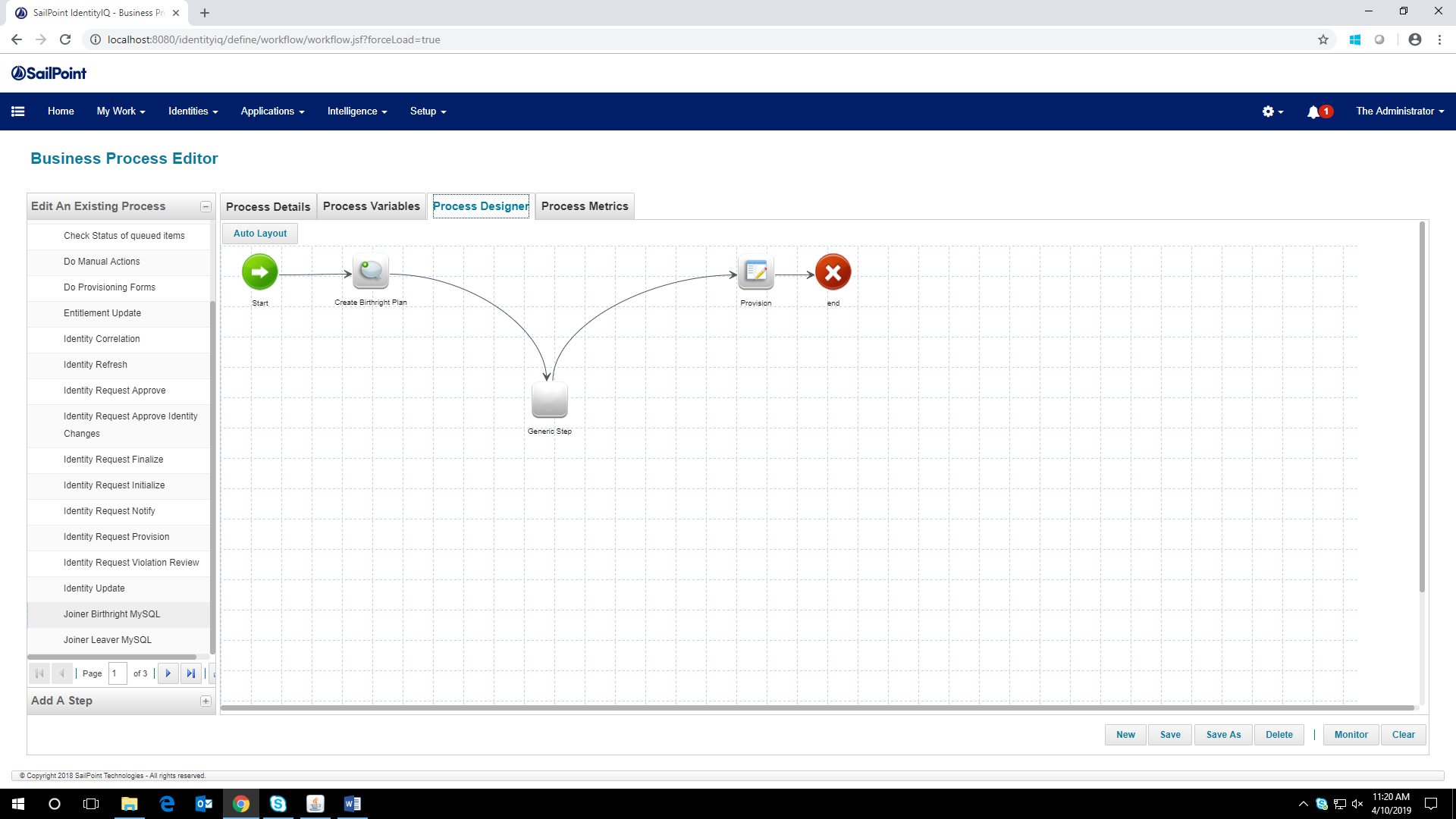
Five lifecycle events are created as shown below (figure --):

* **Manage transfer:** The events get triggered whenever a manager is transferred.
* **Joiner:** Whenever a new identity is created joiner event is triggered.
* **Leaver:** Whenever there is a status(attribute) change this event get triggered leading to removal of user from SailPoint and target system.
* **Reinstate:** Whenever there is a status(attribute) change this event get triggered leading to adding a user which is deleted from target application and SailPoint.
* **custom\_leaver:** Whenever one user status has been changed to inactive both the target application accounts have been disabled through this lifecycle events.
* **Form Updation:** Through this lifecycle one workflow is launched whenever any user tries to change the details of his college or batch and changed or updated value can be shown in his identity because of this lifecycle event.

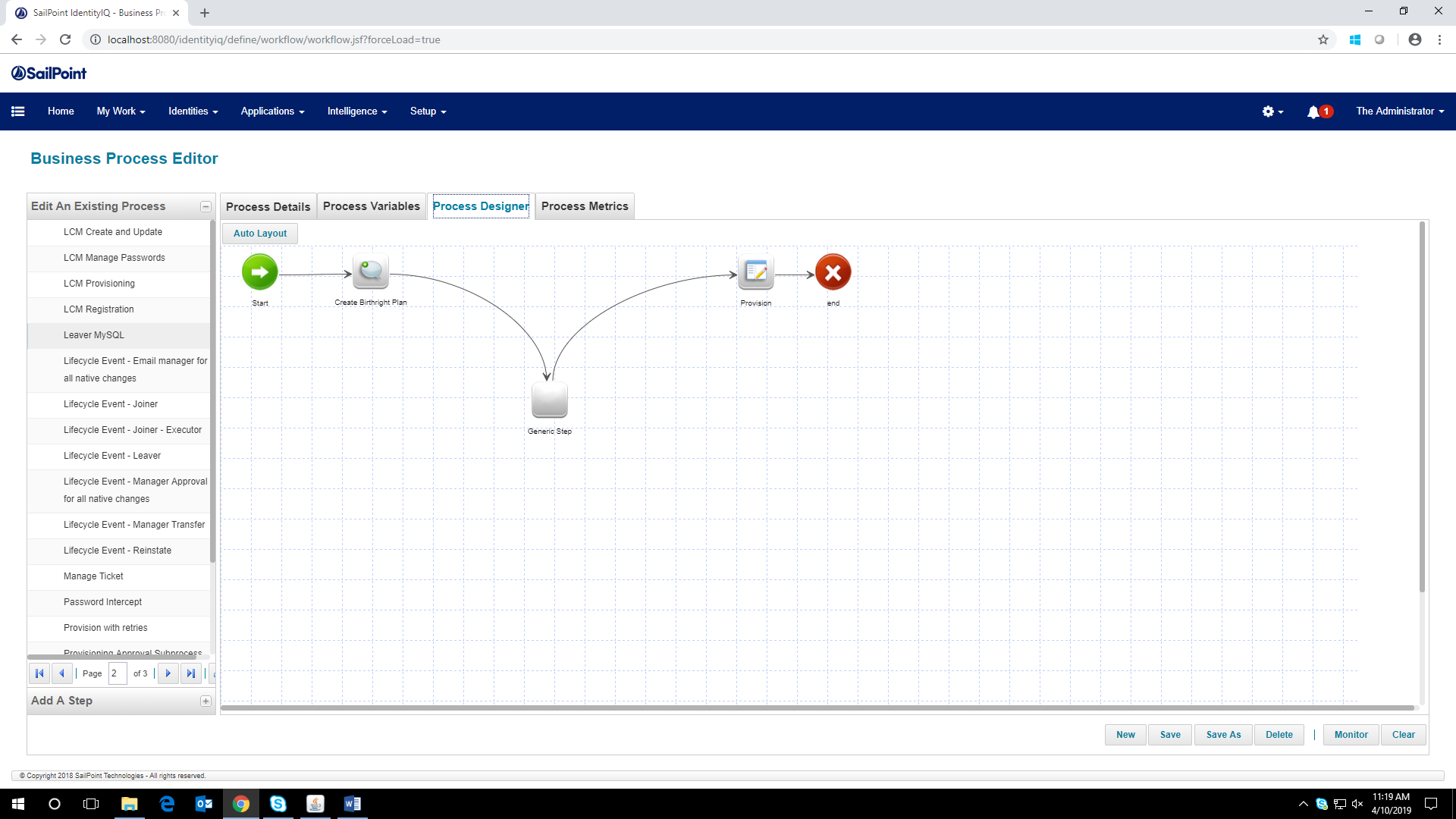


6.6.1. Lifecycle Events

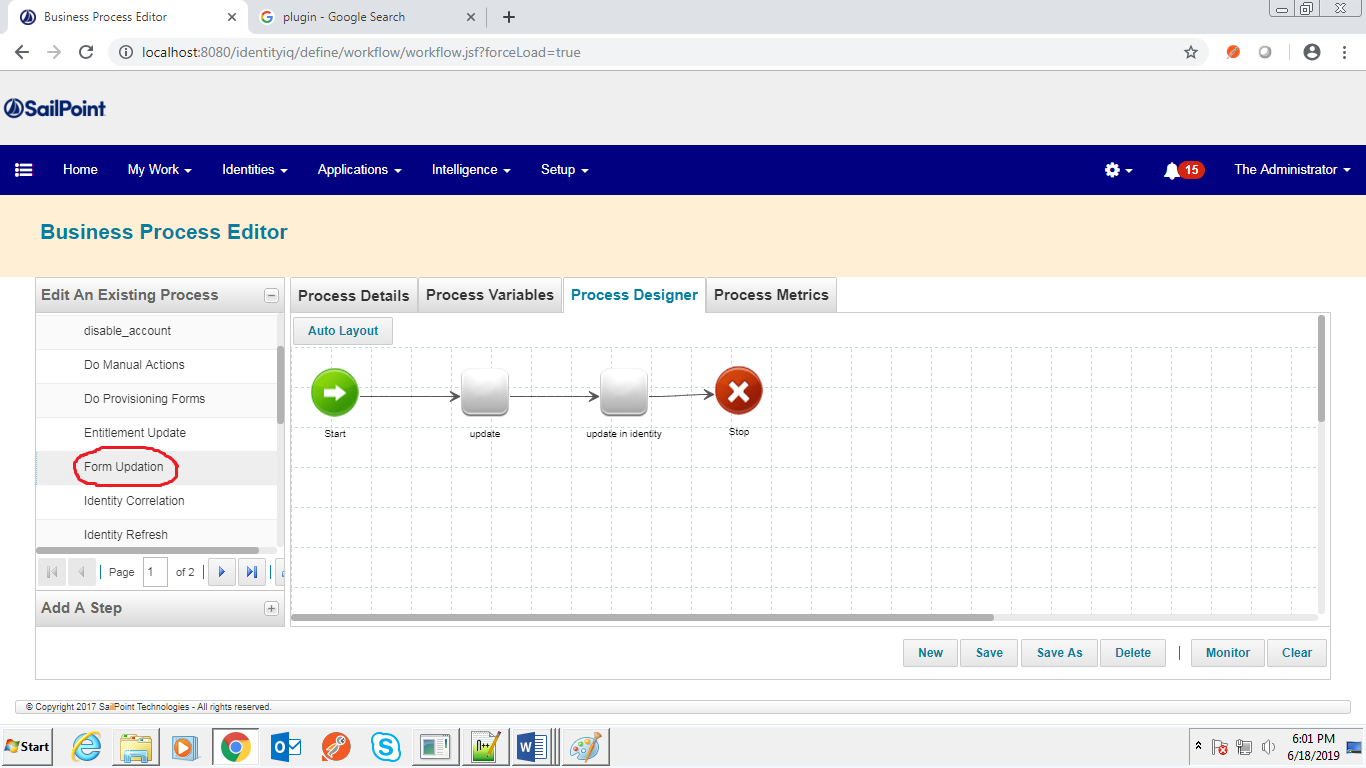
The business process for joiner, leaver, custom\_leaver and access update via form is given in the figures below.



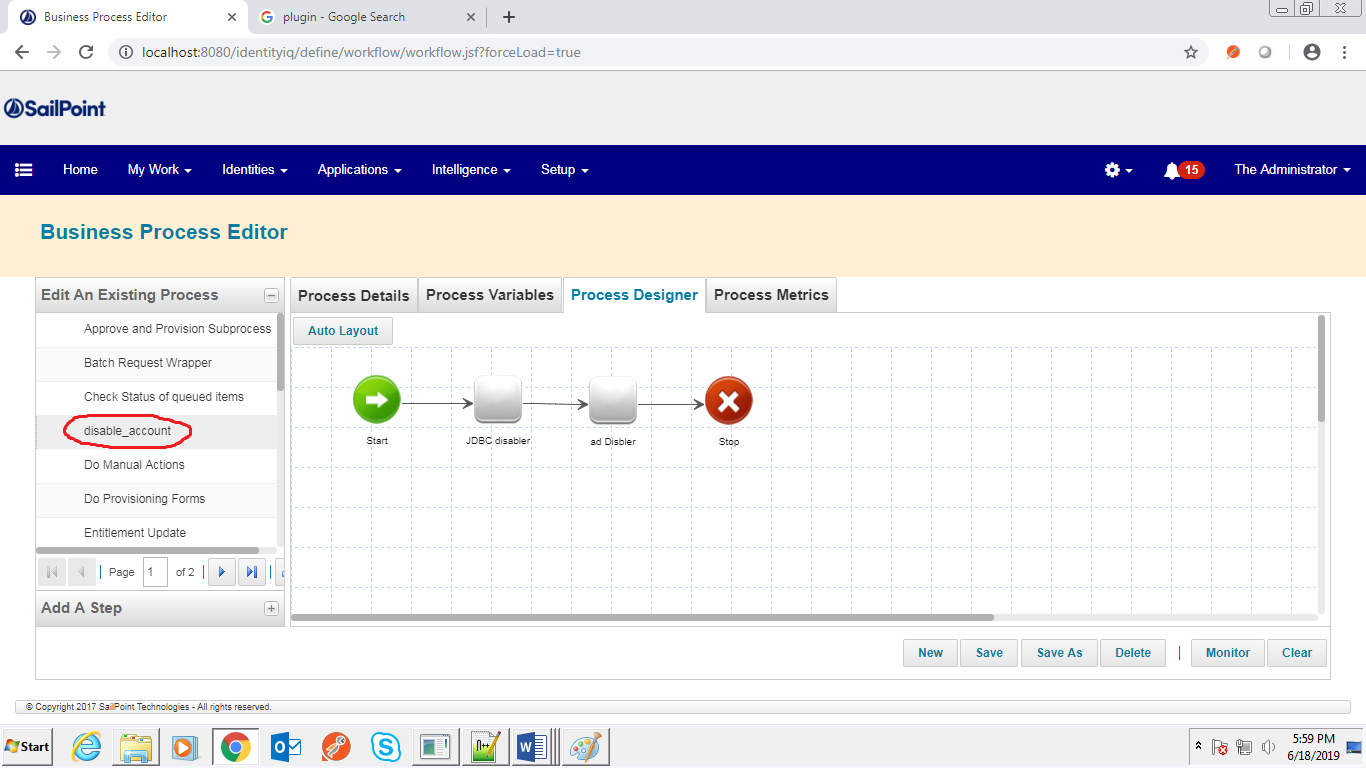
6.6.2. Joiner



6.6.3. Leaver



6.6.4. Access Update via Form



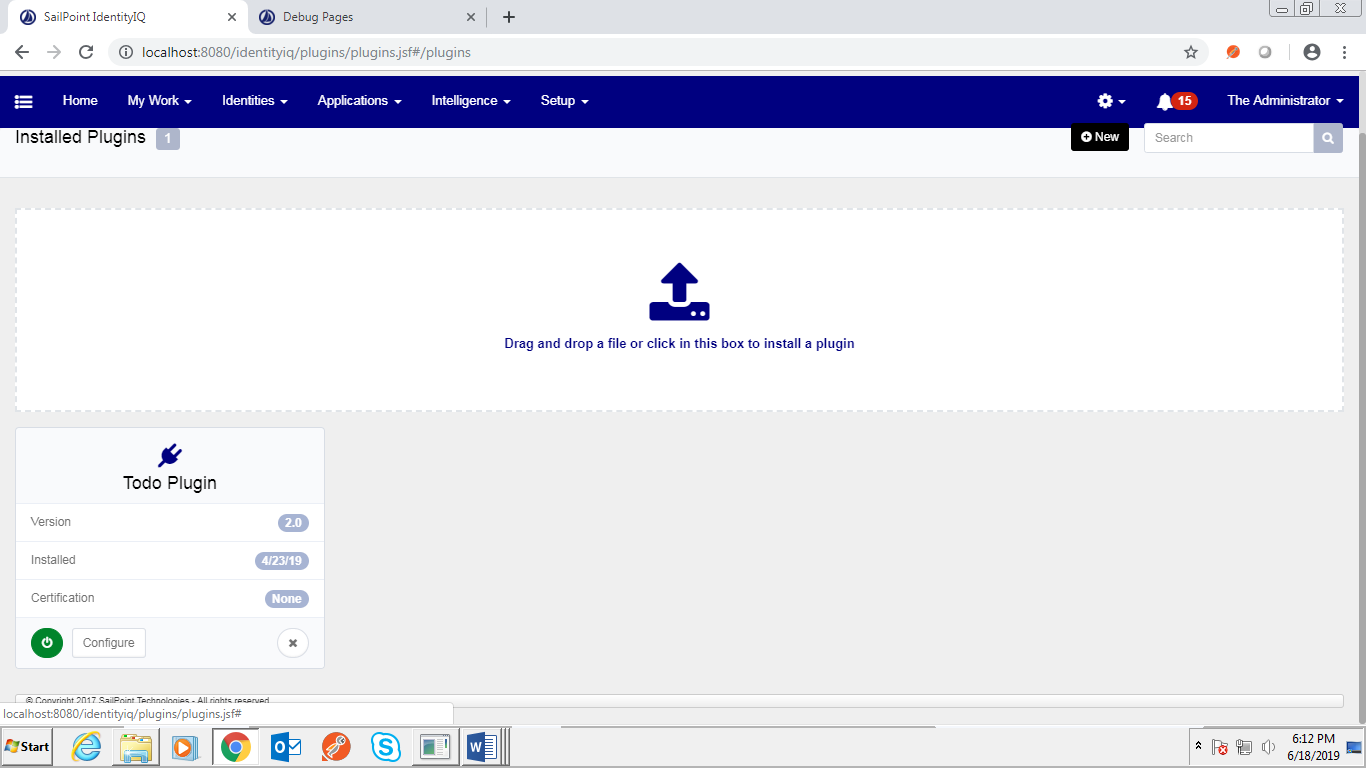
6.6.5. Custom Leaver

* 1. Web Service connector-based application

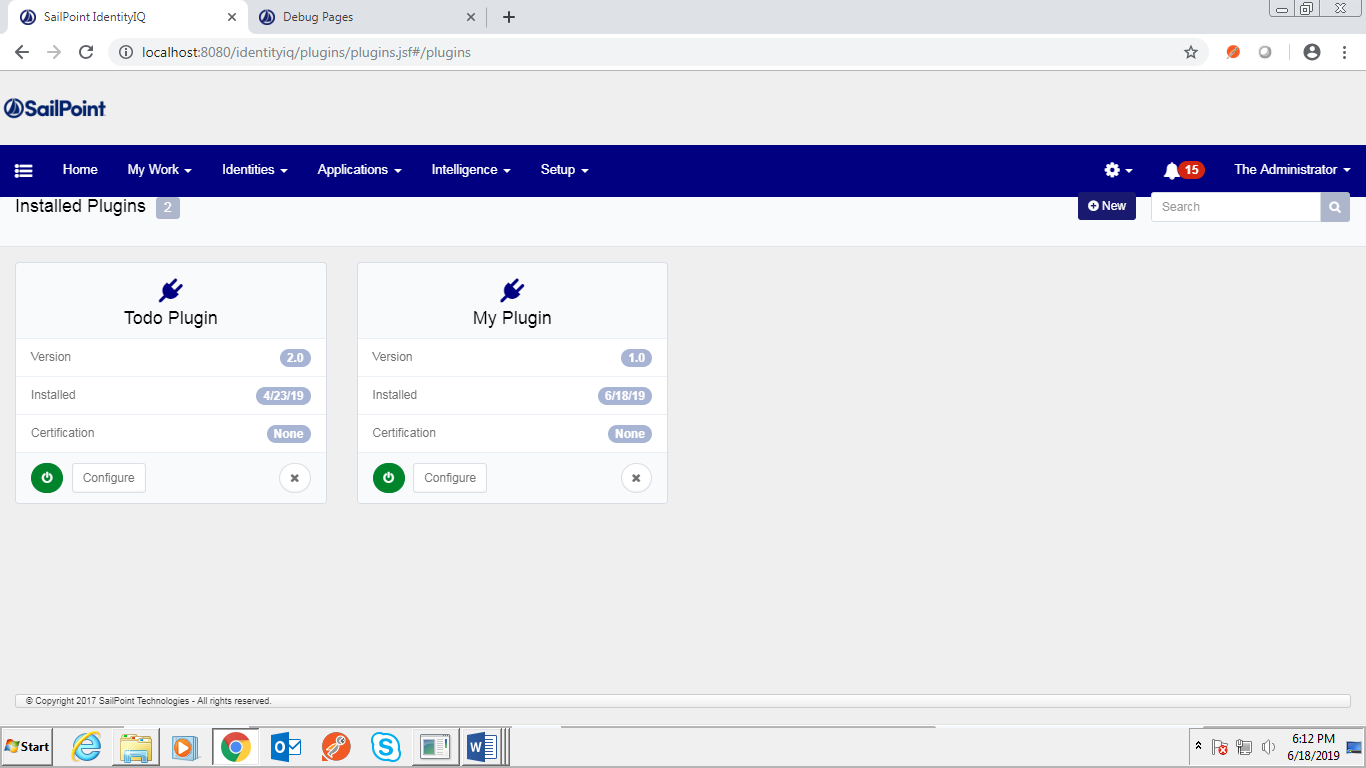
In this field one application was created using SailPoint web service connector which is ***“Custom Web”***. For this application we have to write a java code which will includes the functionality of the application i.e. how the application will work. Every different functionality is defined under different methods. To use those methods in our application we will make a REST calls for every function. So, first we have to give a basic URL, authentication, port and condition which will determine when or how user can access the application.

* 1. Plugin

In computing, a plug-in is a software component that adds a specific feature to an existing computer program. When a program supports plug-ins, it enables customization. In SailPoint we can also add plugin like-



After the installation complete the plugin will appear



This plugin creates a button “Bulk Action” in home page and workitems page.

### CONCLUSION

This project helped me in building my skills in a great and interesting software called as ‘SailPoint IdentityIQ’. This software helps in creating custom solutions with SailPoint and provides an overall understanding and in-depth technical skills for performing in a SailPoint product support role. We were easily able to learn the Core features of the Identity, IQ provisioning stack, Architecture, Object model, Work items and approvals, Dashboard, Auditing, Workflow, Email templates, Lifecycle Manager configuration and capabilities. This software can help the world’s largest organizations to mitigate risk, reduce IT costs and ensure compliance. It provides superior visibility into and control over user access to sensitive applications and data while streamlining the access request and delivery process. SailPoint is being used among the top multinationals. The certified SailPoint professionals are earning the best salaries in the market. Due to increasing demand for SailPoint professionals, there are numerous job opportunities available around the world. High salaries are offered for SailPoint professionals compared to other professionals working on different technologies.

Identity IQ Compliance Manager enhances the business to improve compliance and audit performance while lowering costs, through:

* Business-friendly Access Certifications
* Automated Policy Management
* Audit Reporting and Analytics

Identity IQ Life Cycle Manager offers a business-oriented solution to provide access securely and cost-effectively, through:

* Self-Service Access Request
* Automated Provisioning

Identity IQ Password Manager delivers a simple-to-use solution for managing user passwords to reduce operational costs and boost productivity.

* Self-Service Password Management
* Strong Password Policy Enforcement

Identity IQ allows customers to:

* Enable business users to manage access from any device
* Centralize visibility and governance controls to reduce risk
* Boost productivity while reducing costs

Hence, this project helped me learn and expertize in this effective software SailPoint which is used by many of the companies for identity management and access control.

SUMMARY

This project links people, applications, data and devices to create an identity enabled enterprise. SailPoint is a new software in the market and very less people are there who gets an opportunity to work on this software. As this software is trending in the identity and access management solution for businesses of all sizes, hence gaining knowledge about this software and learning it from the scratch gives us a very good opportunity to build our career in this domain. This project mainly focuses on identity administration and access governance system. The principle feature of this project is its ability to support group and role-based access management. This project focuses on learning how to deploy SailPoint on local host, import identities from CSV and complete the provisioning and de-provisioning using JDBC properties. Different workflows were created for an user to join or leave the organization. Many rules were created to maintain the database of the new joiners and leavers in SailPoint and on the target system. Identity and account mappings were used to combine all the identities along with their properties both in SailPoint and in the database. Access management was achieved using forms and Quicklinks through which the entitlement can be updated based on the request of the user. The access can be updated on the basis of our own requirement. This software can provide complete visibility into who is doing what, what kind of risks are present and accordingly allows us to take the action, we can link people, applications, data and devices to create an identity-enabled enterprise. The benefits of the project include automated provisioning and access control to applications and data. The efforts, errors and time are reduced across access requests. We have an accurate access reporting of who has access to what and if the access is appropriate or not. This software can help the world’s largest organizations to mitigate risk, reduce IT costs and ensure compliance. It provides superior visibility into and control over user access to sensitive applications and data while streamlining the access request and delivery process.

#### REFERENCES

1. SailPoint. https://www.sailpoint.com/
2. Community Portal. https://community.sailpoint.com