

Version 2.1

17th April 2023

SSTL Product Platform Component

User Management System

**Functional Specification Document**

# Disclaimer

User Guide

U11 Energy Billing Solution

for

EGSB

7th Sep’2021

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used for copying, only in accordance with the terms of those agreements. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser’s personal use without the written permission of Eppix eSolution Limited.

All trademarks used herein are properties of their respective owners.

Table of Contents

[Disclaimer 2](#_Toc132636179)

[Document Release History 5](#_Toc132636180)

[Circulation Details 6](#_Toc132636181)

[List of Amendments 7](#_Toc132636182)

[1. Introduction 8](#_Toc132636183)

[2. Scope of the System 8](#_Toc132636184)

[3. Solution Overview 8](#_Toc132636185)

[4. System Actors or Stake holders 9](#_Toc132636186)

[5. Dependencies and Change Impacts 9](#_Toc132636187)

[6. Functional Specifications 9](#_Toc132636188)

[6.1. System Entities 10](#_Toc132636189)

[6.2. Modules and Functions Management 10](#_Toc132636190)

[6.2.1. [FR-1] View Modules & Module Functions 10](#_Toc132636191)

[6.2.2. [FR-2] Disable & Enable Modules & Functions 11](#_Toc132636192)

[6.3. Roles Management 12](#_Toc132636193)

[6.3.1. [FR-3] Create Role 12](#_Toc132636194)

[6.3.2. [FR-4] View & Edit Role 13](#_Toc132636195)

[6.3.3. [FR-5] Disable & Enable Role 13](#_Toc132636196)

[6.4. User Management 13](#_Toc132636197)

[6.4.1. [FR-6] Create User 13](#_Toc132636198)

[6.4.2. [FR-7] View & Modify User 14](#_Toc132636199)

[6.4.3. [FR-8] Suspend User 15](#_Toc132636200)

[6.4.4. [FR-9] Reactivate User 15](#_Toc132636201)

[6.4.5. [FR-10] Delete User 15](#_Toc132636202)

[6.4.6. [FR-11] Password Reset 15](#_Toc132636203)

[6.4.7. [FR-12] Password Policy 16](#_Toc132636204)

[6.5. User Authentication 16](#_Toc132636205)

[6.5.1. Access Control Flow for local users 16](#_Toc132636206)

[6.5.2. Access Control Flow for SSO users 17](#_Toc132636207)

[6.5.3. [FR-13] Login 18](#_Toc132636208)

[6.5.4. [FR-14] Forgot Password 18](#_Toc132636209)

[6.5.5. [FR-15] Change Password 19](#_Toc132636210)

[7. System Configurations 19](#_Toc132636211)

[8. Other System Requirements/ Non-Functional Requirements 19](#_Toc132636212)

[8.1. Audit Trail 20](#_Toc132636213)

[9. Reporting Requirements 20](#_Toc132636214)

[10. Integration Requirements 20](#_Toc132636215)

[11. Data Migration Requirements 21](#_Toc132636216)

[12. Assumptions 21](#_Toc132636217)

[13. Open Items 21](#_Toc132636218)

[14. Out of Scope 21](#_Toc132636219)

# Document Release History

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sl# | Ver. No. | Release Date | Prepared By | Reviewed By | Approved By | Reasons for New Release |
| 1 | 1.0 | 17-Feb-2023 | Saheb Biswas | Abhra Chandra | Abhijit Guhathakurta | Initial Document |
| 2 | 2.0 | 13-Apr-2023 | Rakesh Singh | Abhra Chandra | Abhijit Guhathakurta | Change as per last discussion & comments from Rajiv Jain |
| 3 | 2.1 | 17-Apr-2023 | Rakesh Singh | Abhra Chandra | Abhijit Guhathakurta | Inclusion of User Self onboarding process |

# Circulation Details

|  |  |  |
| --- | --- | --- |
| Copy No. | Designation of Copy Holder | Location of the Copy |
| 1 | Eppix Project Manager | Soft Copy in SVN |
| 2 | SSTL Project Manager | Soft Copy via Email |

# List of Amendments

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Sl# | Ver. # | Section No. /Page No. | Description of the amendment | Raised by | Response | Updated By | Approved by |
| 1 | 2.0 | All doc | Change as per last discussion & comments from Rajiv Jain | SSTL | Updated FS document | UMT | SSTL |
| 1 | 2.1 | 6. Functional Specifications / Page-9  [FR-6] Create User / Page 13 & 14  [FR-7] View & Modify User / Page 14 & 15 | Inclusion of User Self onboarding process | SSTL | Updated FS document | UMT | SSTL |
|  |  |  |  |  |  |  |  |

# Introduction

This document provides requirement specification for the User Management System for the SSTL platform of products or modules. This document provides detailed information on how the user management system will function and how it will be integrated with other products/modules. This document is created based on the high-level requirements discussed with SSTL and provides traceability on the functional specifications back to the business requirements.

# Scope of the System

The proposed User Management system or module is a standalone application which is a centralize repository of all SSTL products platform’s users and provides the capabilities to validate and authenticate users across products. The scope of the system is –

* Capabilities to define and manage users, roles and modules
* User lifecycle management including onboarding, suspension, reactivation, password change, and password reset and forgot password.
* To provide Role based access control mechanism
* To centrally provide authentication services to all the SSTL platform modules
* To support both native user id and password-based authentication as well as SSO integration via third party OAuth2 or OIDC integrations, i.e. Azure AD, Google login etc.

# Solution Overview

User Management system will be a standalone web passed application. It will provide a web portal (web based application) to configure and manage the system. An administrator user will have access to the portal to configure the system and add more users.

It will publish integration interfaces for all future SSTL platform applications to integrate and validate users and eliminate the need of managing user’s module product wise.

It will support both local authentication (based on user id and password defined on the system) and authentication via SSO integration.

Note:

* Client specific admin access: Each client's instance will be running on a separate environment (may be AWS partitions or containers). Hence complete environment separation will be there.

# System Actors or Stake holders

Following are the identified stakeholder groups / users in the system

| User/Role | Example | Frequency of Use | Security/Access, Features Used | Additional Notes |
| --- | --- | --- | --- | --- |
| Administrator |  | Frequent | System configuration, User and roles management etc. | Only one admin user per client / installation. |
| User |  | Most Frequent | Authentication, Forgot Password, Change Password etc. |  |

# Dependencies and Change Impacts

User management module will not have dependencies on any other SSTL platform products; rather other platform modules will be dependent on this module.

As this is a new module there is no change impact. Once other platform products are built, they need to be integrated with this module.

# Functional Specifications

Following are the features of the User Management module. Each functionality of the module is identified by a unique FS# which provides traceability across documents for the said functionality.

| Serial# | Functional Area / Process | Detailed Functionalities / Use Cases | FS # |
| --- | --- | --- | --- |
| 1 | Modules & Functions  Management | View Modules & Module Functions | FR-1 |
| 2 | Disable & Enable Modules | FR-2 |
| 3 | Roles Management | Create Roles | FR-3 |
| 4 | View & Edit Roles | FR-4 |
| 5 | Disable & Enable Roles | FR-5 |
| 6 | User Management | Create User &  User Self Onboarding | FR-6 |
| 7 | View & Modify Users | FR-7 |
| 8 | Suspend User | FR-8 |
| 9 | Reactivate User | FR-9 |
| 10 | Delete User | FR10 |
| 11 | Password Reset | FR-11 |
| 12 | Password Policy | FR-12 |
| 13 | User Authentication | Login | FR-13 |
| 14 | Forgot Password | FR-14 |
| 15 | Change Password | FR-15 |

# System Entities

Following are the main system entities for this User management module.

* **Modules** – Modules are the software components or products which will be built as part of the SSTL platform. For example ATS is a module. Access to all these modules will be controlled via this user management module.
* **Functions** – Functions are the unit of functionalities inside a module or any sub-module/feature of it. For example ATS can have a function for “creating a site”. Access control mechanism works on these functions. Privileges on these functions are either provided or taken off to/from the users. Functions are specific to modules.
* **Roles –** Roles are collection of module wise functions defined to control user access to one or multiple modules. Roles can be defined using multiple modules and functionalities.
* **Users –** Users are the entities who have access to the different modules and functionalities and operate the system as per their privilege of the system.

# Modules and Functions Management

# [FR-1] View Modules & Module Functions

Modules are auto configured and automatically available in the user management system when the corresponding software component is deployed. Each software component or product (i.e. ATS) is a module. When deployed in an environment the module entity for that product is auto created in User management module. Each module entity consists of

* an unique ID
* Module Code
* Module Description

The module entity in User management cannot be manually created rather only available if the corresponding software component is deployed in that environment.

In the same way, functions of a module are also auto configured and automatically available in the user management system when the corresponding module is deployed. Each functions of a module are unit of functionality on which privilege can be given or taken away. The functionalities referred here are mapped with back end functional APIs. So functions are linked with APIs. Each function entity consists of

* an unique ID
* Function Code
* Function Description

The functions entity in User management cannot be manually created rather only available if the corresponding module is deployed in that environment.

The mapping between a Module and it’s functions are pre-defined as part of the corresponding product (i.e. ATS).

A GUI to view the modules and module wise functions will be provided. The GUI will be read only, i.e. no field will be editable.

# [FR-2] Disable & Enable Modules & Functions

A deployed module can be disabled in an environment to make it unavailable for role configuration. In the same way it can also be enabled to make it available for role configuration. Also functions under a module can also be disabled or enabled to make them available/unavailable during role creation.

The same GUI to view module and it’s functions will have options to enable or disable modules and functions. Once a module or a function under a module is disabled, it cannot be selected during new user roles creation.

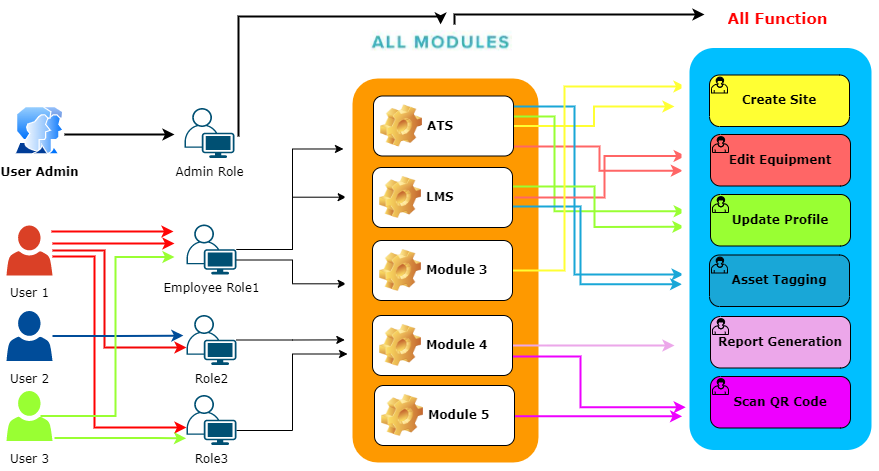
Any existing user roles previously created using the recently disabled module functions will continue to have access to that module or function. In other words, disabling a module or function does not affect the existing roles created using that module or function.

Once a module is disabled from User management system, the same module will not be accessible to the user on next login.

# Roles Management

Role management is the process of controlling what functionalities are available to a user under a particular module by associating that information with a role. Hence admin or other users will have accessibility based on the role assigned.

Roles enable systems to allow access only for the specified functionalities to users. System will allow creating as many roles as required using the deployed modules and functions.



**Figure – User > Role>Module>Function Concept Diagram**

Roles are associated with users. One user can have multiple roles associated with it. So the user eventually will have cumulative privileges from all the roles assigned to.

A role entity consists of following –

* an unique ID
* Role Code or Name
* Description of the Role
* Modules & Functions associated with the role

# [FR-3] Create Role

A screen will be provided for creating a new role. Role Name or Code will be unique. It will provide option to assign modules and functions to a role. User may assign one or modules and functions to a role. There should be option to add all or selective modules and functions to a role.

# [FR-4] View & Edit Role

All the roles will be visible in a tabular / list view. The details of a role (Modules and Functions) will be visible. User may add/remove modules and functions to a role and update the role. Role Code or name cannot be updated.

# [FR-5] Disable & Enable Role

In the view role GUI, user can enable or disable any role. Once the role is disabled or enabled the user access control will be changed accordingly.

# User Management

# [FR-6] Create User

The create user section will have feature to add new user. This option will allows creating a new user based of different attributes and upon associating the required role and other details. Multiples roles can be assigned to a user. User can be created without any role and roles may be added later.

A user entity will consist of –

* User id (Unique identifier of a user. Also used to login)
* User Name
* Address
* Email (Unique. To be used for Email OTP based login)
* Mobile (Unique. To be used for SMS OTP based login)
* Alternate Contact Number
* Roles assigned to the user
* Authentication Source (Local or SSO)

For users with authentication source set to local - Once the new user is added a notification will be triggered to the user via email and SMS with the user id and auto generated password. The password validity should not be more than 10 minutes. On the first login attempt user must be forced to change the password.

For users to be authenticated by SSO no email needs to be sent.

All users created are by default in active status except for Self on-boarding.

Multiple roles can be assigned to a user.

**User Self Onboarding:**

Alternatively, there would be an option for User-Self Onboarding from User Management Login screen for Self-Registration. System user needs to provide registration inputs:

* User id (Unique identifier of a user. Also used to login)
* User Name
* Address
* Email (Unique. To be used for Email OTP based login)
* Mobile (Unique. To be used for SMS OTP based login)
* Alternate Contact Number

Once submitted, the user will be created in PENDING state. Subsequently, Admin or authorized user can activate the newly created user followed by assigning proper role as required.

# [FR-7] View & Modify User

All the available users can be viewed in list/tabular format. Option will be there to search /filter users based on user attributes and status. Details of a particular user should be viewable along with the role assigned to it. Following attributes of the user should be visible –

* User id
* Name
* Address
* Email (Unique)
* Mobile (Unique)
* Alternate Contact Number
* Roles
* Authentication Source (Local or SSO)
* User Status (Active, Pending, Blocked, Locked, Deleted)
* Last Password Change Date
* Password Expiry Date
* Password Reset Flag
* Number of Failed Login attempts
* Last failed log-in attempt
* Last successful log-in attempt

In this section Edit User option will also be there. Once it is clicked the User details option will appear with all user details and user roles. If admin wants to change any information then he can only able to change the below attribute and save modified details.

* User Name
* Address
* Email (Unique)
* Mobile (Unique)
* Alternate Contact Number
* Roles
* Other attributes

New roles can be added or existing roles removed.

There will be an option to activate a pending user which can be done by an authorized user.

User’s authentication source can also be changed. In case authentication source is changed from SSO to local, password needs to be auto generated and communicated to the user via Email/SMS. User must be forced to reset the password during next login.

# [FR-8] Suspend User

From the user details view a user can also be suspended or blocked. Remarks/Reason for blocking needs to be entered. Blocked users will not be able to login or authenticate themselves or reset password via ‘Forgot Password’ or change password.

# [FR-9] Reactivate User

A suspended user can also be reactivated from the user details view. Users reactivated can again perform all operations as per their role.

# [FR-10] Delete User

From the user details view a user can also be deleted. Once a user is deleted the user loses all access (login, logout,. Deleted users cannot be revived. The user id cannot be reused.

# [FR-11] Password Reset

It is possible to reset password for users who have authentication source set as ‘Local’. Once a password is reset for the user a new randomly generated password is sent to the user via Email/SMS. The validity of such password should not be more than 10 minutes. User must be forced to change the password on the next login.

Users who are blocked or deleted, their password cannot be reset.

# [FR-12] Password Policy

**Dynamic Password Policy** - Dynamic password policy needs to be supported. Following password parameters should be configurable as per business need –

* + Min length of Password
  + Max Length of Password
  + Min Number of lowercase alphabet
  + Min Number of uppercase alphabet
  + Min Number of digits
  + Min Number of Special characters
  + Password Expiry Duration
  + Consecutive number of failed login attempts to lock User id
  + Authentication token expiry duration

Last 5 passwords of a user need to be maintained and cannot be used. Password expiry date needs to be maintained and user must be forced to change the password on password expiry.

# User Authentication

This module will support two mechanisms for user authentication.

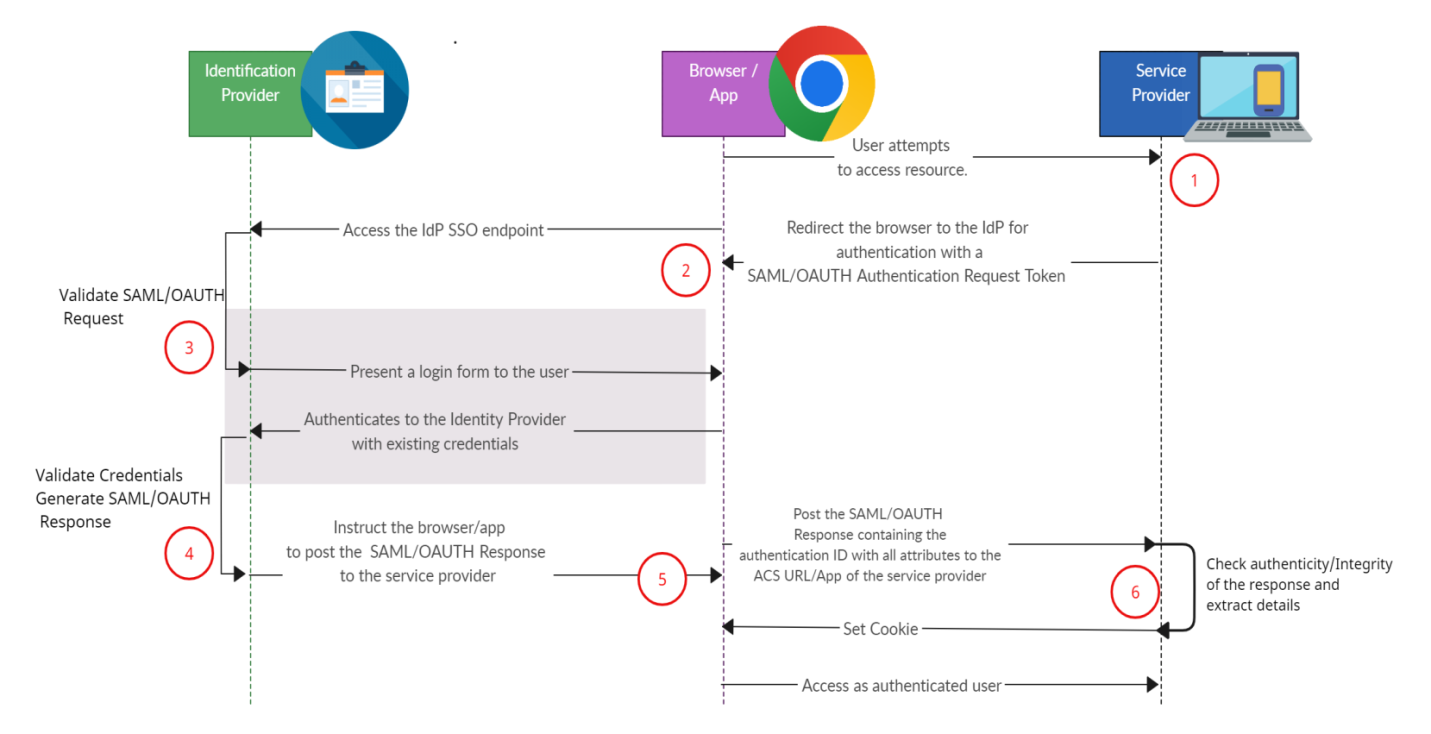
* Local – User Id and Password based authentication
* SSO – Third party OAuth2 based authentication

# Access Control Flow for local users

The users who have the authentication source set as local, they need to enter user id/mobile no/email id and password for authentication. Once successfully authenticated, the system generates a token containing the user details (along with privileges). The token is set as a domain cookie. This token is used for all future requests by the user. Once the token is invalidated or expired the user needs to re-authenticate again to generate a new token.

# Access Control Flow for SSO users

The flow of user access control and authentication process will be conceptualized like below.



**Figure – User Access Authentication Flow Diagram**

* The user will initiate the authentication flow by clicking a login button or by visiting a secured area of the web application. The web application generates a SAML/OAUTH message known as a SAML/OAUTH Authentication Request because SAML/OAUTH authentication is configured for the web application. This message is the request to an identity provider to authenticate this user.
* The user's browser is forwarded to the Identity Provider with the compressed and Base64-encoded Authentication Request message as an HTTP GET parameter.
* After confirming that the Authentication Request originated from a Service Provider it trusts, the Identity Provider asks the user to authenticate, usually by filling out a login form.
* The user authenticates with the Identity Provider using their existing credentials and if successful, the Identity Provider proceeds to create a SAML/OAUTH Response message that contains a SAML/OAUTH Assertion. In essence, by constructing the SAML Assertion, the Identity Provider asserts that this user has authenticated successfully and they are known to have certain characteristics that are released in the form of SAML/OAUTH Attributes and their values.
* The Identity Provider, then, instructs the user’s browser to make an HTTP POST request to the URL where the Service Provider expects SAML/OAUTH Response messages, called the Assertion Consumer Service URL, with the SAML/OAUTH Response Base64 and URL encoded in the body of the request.
* Finally, the Service Provider receives the SAML/OAUTH Response to the SAML Authentication Request it had originally created and after verifying its authenticity and integrity, “consumes” it in order to retrieve the fact that the user has been successfully authenticated and the information about that user’s identity in the form of attributes. It then passes this information to the web application for it to create a session for the user.

The application will issue an access control error if the user authentication fails and their identity does not match.

# [FR-13] Login

Any attempt to access any protected resources of User Management module or any other SSTL platform modules (i.e. ATS) will redirect the user to a Login page. This login page end point will be published by the User management module. User needs to enter the user id or mobile number or email id and click next. System will check if the entered user id/email id /mobile no. exist and what is the authentication source. In case the authentication source is local, user will be prompted for password. But in case the authentication source is SSO, user will be redirected to the authentication provider page (i.e. Azure login).

Once successfully authenticated the user will be redirected to the protected resource originally attempted to access via URL redirection. (See [Section 10 – Integration Requirements](#_Integration_Requirements))

Suspended or deleted users will not be able to authenticate themselves. Users for whom password has been reset or password is expired or logging in for the first time they will be first forced to change their password, and then only redirected to the protected resource originally attempted to access.

In case of consecutive failed login attempts, system must inform user about number of attempts remaining before user is locked. Also captcha based validation will be there to prevent brute force attack or login by robots.

# [FR-14] Forgot Password

In the login page itself an option for Forgot Password use case will be provided. If users have forgotten their password, users can reset their password either through email based or mobile number based OTP. Users need to enter wither their mobile number or email. The entered mobile or email id should be same as on record for that user. The password is reset and auto generated password is sent to the email or SMS. The validity of the password will be max 10 minutes. On successful authentication with the password system should force the user to change password.

Forgot password is only applicable for users having authentication source set at Local.

# [FR-15] Change Password

User management module will publish an endpoint for Password change for authenticated users. Users need to enter their old password, new password and retype new password. The password should be validated against the password policy configured. This will be only available for users whose authentication source is local. The URL for password change needs to be integrated in the other platform modules (i.e. ATS) as URL redirection or iframe integration.

Change password is only applicable for users having authentication source set at Local.

# System Configurations

* **SSO Configuration** - Following system level configuration will be provided for SSO configuration (OAuth2 or OIDC). This will be implementation specific configuration done once during implementation.
  + Token URL
  + Authorization URL
  + Client Id
  + Client Secret
* **Dynamic Password Policy** - Dynamic password policy needs to be supported. Following password parameters should be configurable –
  + Min length of Password
  + Max Length of Password
  + Min Number of lowercase alphabet
  + Min Number of uppercase alphabet
  + Min Number of digits
  + Min Number of Special characters
  + Password Expiry Duration
* Consecutive number of failed login attempts to lock User id
* Authentication token expiry duration

# Other System Requirements/ Non-Functional Requirements

* Availability of APIs for all user operations
* Availability of detailed log files for all operations
* Pagination on all tabular views and lists
* There should be traversable links on all reference to the main entities of the system (Role, Function and User). For example if in a GUI view user details is being shown and it is showing roles of the user, then those roles should be navigable, meaning clicking on the role will take the user to the role view GUI.
* Any URL redirection (in case of authentication success and failure) from the user management module should not happen outside the current domain.

# Audit Trail

System will capture all types of events which can show who did, what activity happened and when. The administrator will examine all types of change logs to get a complete picture of normal and abnormal events on the user management system.

* + - The following fields will be captured for each event performed by a User

|  |  |
| --- | --- |
| **Field Name** | **Details** |
| Event id | UUID |
| Event Name | What action performed |
| Modified By | Who performed |
| Modified On | When performed |
| Description | Event details if any |
| Attribute Name Value Pair | A list of attribute name value pairs for attributes which were changed |

# Reporting Requirements

* None

# Integration Requirements

* Integration capability with SSO provider using OAuth2 or OIDC protocol to be provided.
* Integration mechanism for SSTL platform products (modules) for authentication and user management to be provided.
  + User management module should expose web URLs where other modules will be able to redirect for authentication.
  + User management module should accept success and error URLs as URL parameters from the integrating modules, so that it can redirect to those URLs according to the authentication success or failure.
* Email gateway integration
* Google reCaptcha integration

# Data Migration Requirements

* None (To be scoped in project implementation phase)

# Assumptions

* Maximum one SSO provider will be supported per implementation.
* OAuth2 and OIDC will be supported as SSO integration mechanism.
* In the case of SSO integrations all the users in SSO platform also need to be maintained in this module. The roles and access control will apply based on this module’s configuration.
* Email notifications will go to user's email. If user has set GMAIL, notifications will go there. There should not be any Email domain enforcement.

# Open Items

* None

# Out of Scope

* SMS Gateway integration is out of scope and will be scoped during project implementation.
* License management is not in scope of User Management.