



# Password Manager Discovery Documentation



**Questions?**

Contact us at [engage@unified.com](mailto:engage@unified.com)

## Table of Contents

<b>1. Introduction</b> .....	3
<b>2. Client Information</b> .....	3
<b>3. Password Manager</b> .....	4
<b>4. Directory Server Information</b> .....	7
Active Directory Hostname and SSL Port Number .....	7
Choose an item. ....	7
<b>5. Test Accounts for Testing</b> .....	9

## Introduction

This document captures all the details of the client’s project team and prerequisites required for the implementation of Password Manager Module. This information will be used for implementing and configuring the Password Manager module on the client’s Unifyed production environment

## Client Information

Name	Email Address	Phone #	Role	Sub – Contractor

**Roles:**

- 1. Sponsor
- 2. Project Manager
- 3. Portal Administrator
- 4. Back Up Portal Administrator
- 5. Network Administrator

\*Per the CampusEAI Master Services Agreement your institution has executed with CampusEAI, the institution must identify any staff working on the project that are contracted. Contracted staff must receive authorization and execute CampusEAI Confidentiality Agreements in order to receive access to CampusEAI resources.

## Password Manager

Unifyed password manager provides a one stop shop self-service password management experience and comes with below listed module:

### First Time Users workflow:

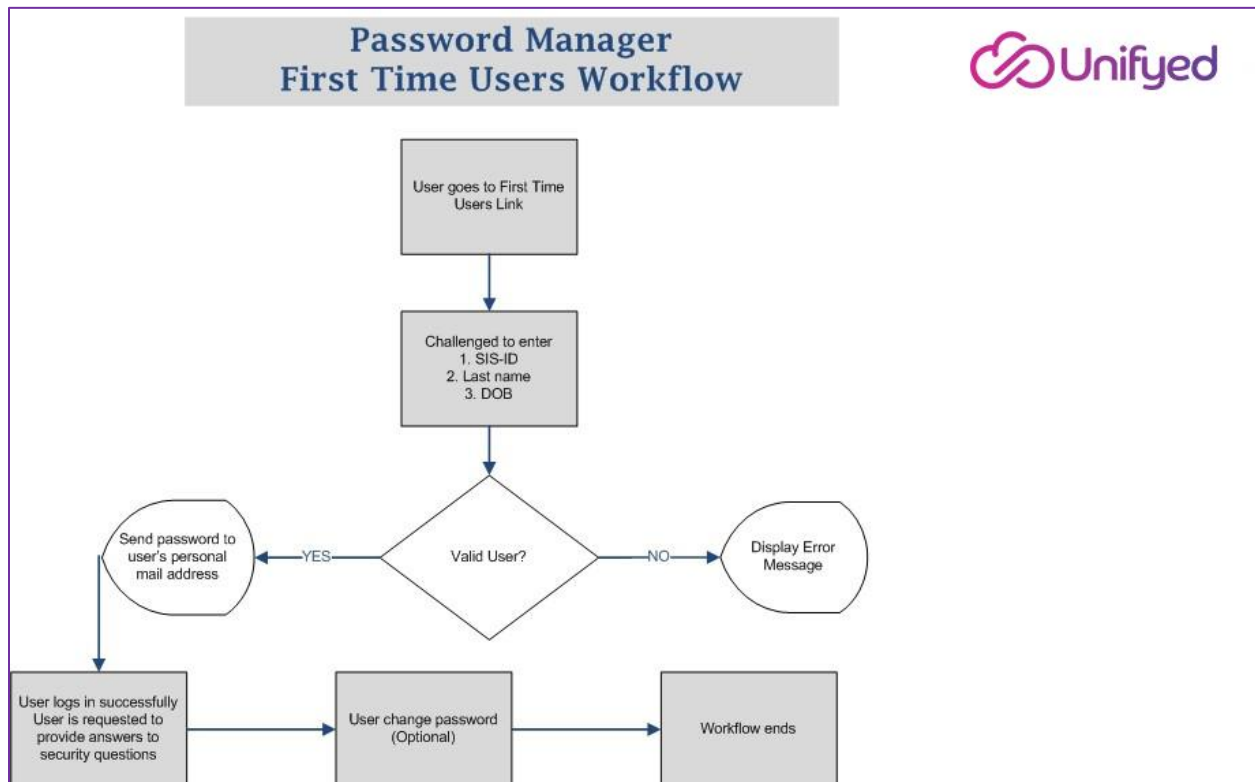
Unifyed password manager provides a first-time users workflow so that all the new users could simply use password manager in order to obtain passwords to all the backend systems that are getting authenticated against institutional directory server.

This helps the overall institutions security as users would no longer need first time passwords over the student center helpdesk counters.

Unifyed uses ERP/SIS system for validating the first-time users and currently validate user's authenticity using:

- Banner / ERP ID
- Last Name
- Role

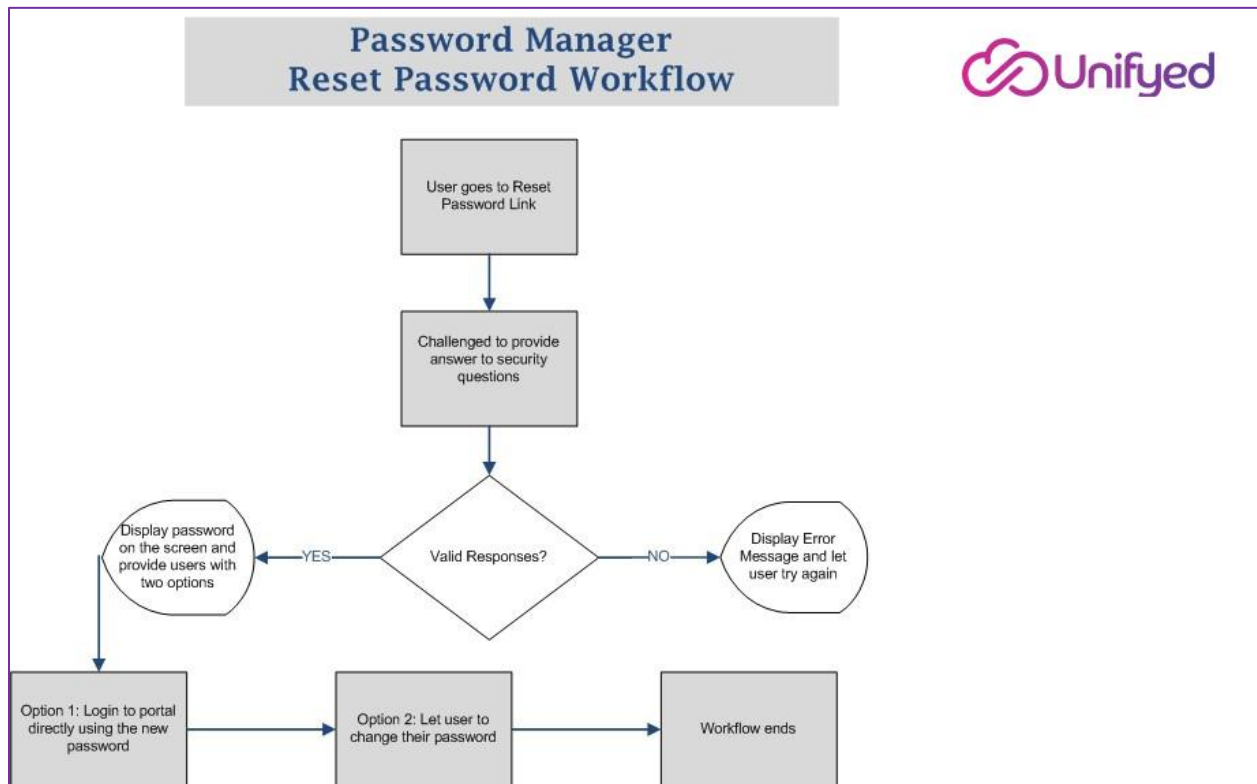
NOTE: We can support custom SIS attributes as well if need be.



## Reset password Workflow

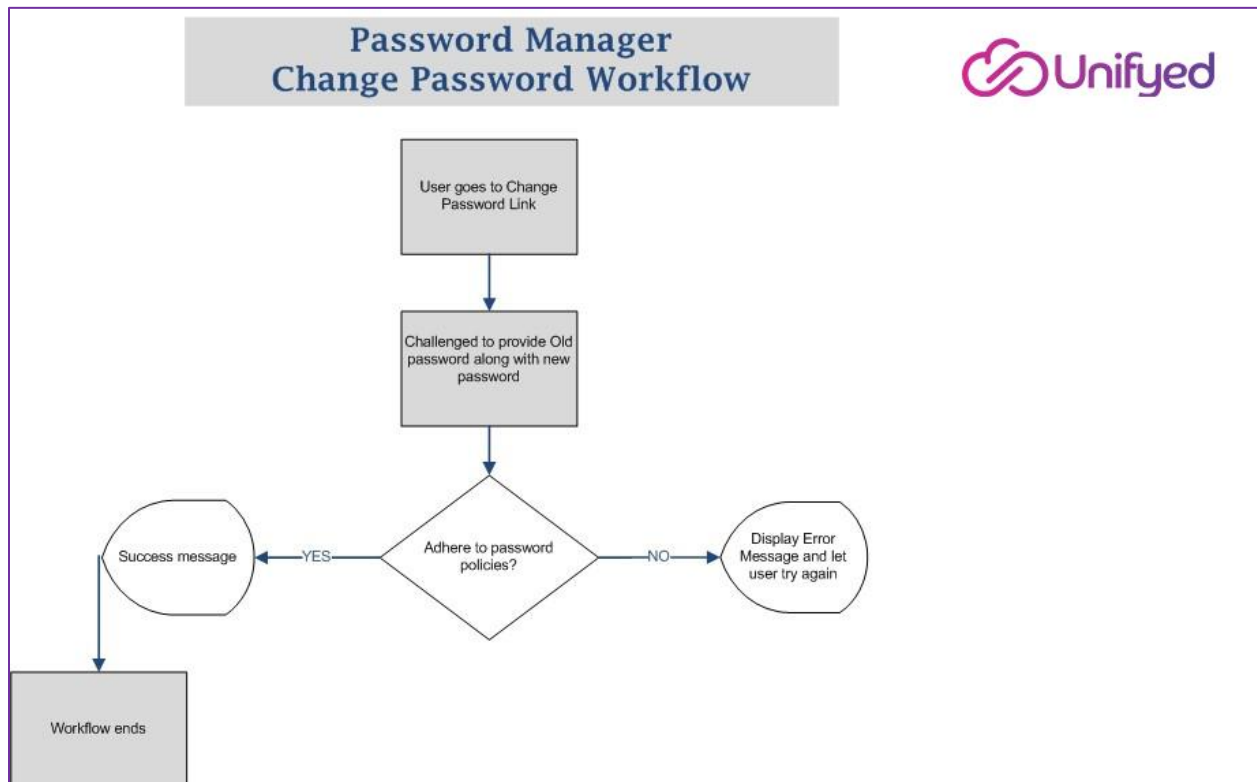
Unifyed password manager provides a reset password workflow so that users can reset their passwords using existing security questions and answers which they must have filled in at first login to Unifyed platform.

User is challenged to answer security questions and have an option to skip them in case they do not remember any responses to the question. Administrations can define the number of answers limit for all the users which is a must to answer before generating new password.



## Change password Workflow

Unifyed password manager provides a change password workflow so that users can change their passwords if need be and also adhere to active directory's password policies and complexities.



## Directory Server Information

AD Server Information	
Active Directory Version	
Active Directory Hostname and SSL Port Number	Choose an item.
AD Bind account name and password  <b>Note:</b> The bind account needs to be granted privileges to update "unicodePwd" attribute for password updates	
Password History Control (1.2.840.113556.1.4.2066) availability in Active Directory?	
Password Policy Information	

Password History?	
Minimum password age?	
Maximum password age?	
Minimum password length?	
Password complexity requirements?	

First Time Users Validation	
Attribute for User ID	
Attribute for Last name	
Attribute for Role	
Personal Email Address	
Please provide query which will return LDAP ID using above three values (e.g. value typically stored under gobtpac_external_user)	
Please provide query which will return personal mail address of the user using above values	

Banner Server Information	
Banner IP: Test Banner DB Prod Banner DB	
SSL Port Number (Test and Prod Both)	
SSID/Database Name (Test and Prod Both)	



Bind account name and password  <b>Note:</b> The bind account needs to be granted privileges to read the information for the queries.	
---	--

Verification Source (Verification Questions)	
Select the type of verification source that you would like to configure?	<ol style="list-style-type: none"> <li>1. Admin Defined OR</li> <li>2. User Defined</li> </ol>
Description of verification sources <ol style="list-style-type: none"> <li>1. Admin Defined Verification Source:                 Allows Admin to configure a set of pre-defined questions and users are required to answer all those questions post first time login.</li> <li>2. Admin Defined Pooled Verification Source:                 Allows Admin to configure a pool of questions and users get the flexibility to select the questions from the dropdown.</li> <li>3. User Defined Verification Source:                 Allows user to create their own custom questions and answers.</li> </ol>	

Custom Messages	
What should the notification mail subject be when user uses first time user's option?	
Who should be the sender of the mail when user uses first time user's option?	
What should the message body be when user uses first time user's option?	

## Test Accounts for Testing

USER ID	Firstname	Lastname	Description	physicalDeliveryOfficeName

**Disclaimer**

Any changes made in the information provided in this document by the member school post the sign-off (during the course of the project implementation) needs to be approved by Campus Consortium as it may have impact on the scope, timeline and cost of this project.

**Client Project Lead**

_____	_____
Authorized Name	Date
_____	_____
Authorized Name	Date

**Unifyed Identity Delivery Lead**

_____	_____
Authorized Name	Date
_____	_____
Authorized Name	Date