Enterprise Self-Service Portal

FAQ

General Information: **info@cionsystems.com**

Online Support: **support@cionsystems.com**

CionSystems Inc.
6640 185th Ave NE
Redmond, WA-98052, USA
http://www.CionSystems.com
Phone: +1.425.605.5325

Trademarks
CionSystems, CionSystems Inc., the CionSystems Inc. logo, CionSystems Active Directory Manager Pro are trademarks of CionSystems. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Copyright 2017 CionSystems Inc., All Rights Reserved

Table of Contents

Copyright 2017 CionSystems Inc., All Rights Reserved

General Information

Q: How do I configure Enterprise Self-Service Portal?

A: Before using Enterprise Self-Service portal administrator must configure the application. There is a 4 step configuration to Enterprise Self-Service deployment.

1. Configure the application to talk to an Active Directory domain in the back end. You do this by login to the Enterprise Self-Service application via "administrator page" by providing username – 'admin' (without quotes) and password 'admin' (without quotes). With first time install and configuration, you will see an option to configure "local domain". Please provide "high privilege" active directory account, preferably an account with administrative privileges. Configure the domain and the domain-controllers, mark the primary domain controller.
2. Once the Enterprise Self-Service successfully connects to active directory domain you will see "dashboard" which provides insight into active directory users and Enterprise Self-Service state.
3. Now you are ready to configure self-update settings, password and account unlock policy and security questions. Please refer to help file for helping configure these options.
4. Send email to user community to enroll with Self-Service. Fill out the invitation and send to the user community.

Q: How do I configure the application to use HTTPS?

A: You can configure Self-Service to use HTTPS by configuring the application in IIS for https protocol. The default install is for http. Before using https, you need to obtain a proper certificate. Refer to "ADS_SSL installation procedure.doc" document

Q: How do I allow remote users to connect the application?

A: You can expose the Self-Service URL to remote users by navigating the http/https traffic and redirecting it to the URL. First configure the URL and map it to a DNS name. Then configure the NAT box to redirect the http/https traffic to Self-Service URL. You can also configure the URL and map it to a publicly accessible IP address. Our recommendation is to use https to connect to Self-Service URL from outside the firewall.

Copyright 2017 CionSystems Inc., All Rights Reserved

Q: What is the default administrator user name and password?

A: The Default credentials of the application are:

Username: admin
Password: admin

Q: What is the default poweruser name and password?

A: The Default credentials of the poweruser are:

Username: poweruser
Password: user

Q: How do I ensure that the users don't see "admin" tab on their home page?

A: Ask user community to connect to
http://localhost/SelfService/frmUserLogin.aspx

Q: How do I connect to "administrator" home page?

A: The administrator home page is http://localhost/SelfService/frmLogin.aspx

Q: How do I configure domains?

A: Enterprise Self-service supports both Microsoft Active Directory and Azure Active Directory. You can't configure both AD and Azure Active Directory domains at the same time. If you need, then you will need separate install one for each Active Directory.

To *Configure a Domain*

- Click on Start Button>All Programs> Enterprise Self Service portal> Enterprise Self Service icon.

  OR

- Click Enterprise Self Service portal Icon on desktop and follow the below procedure.

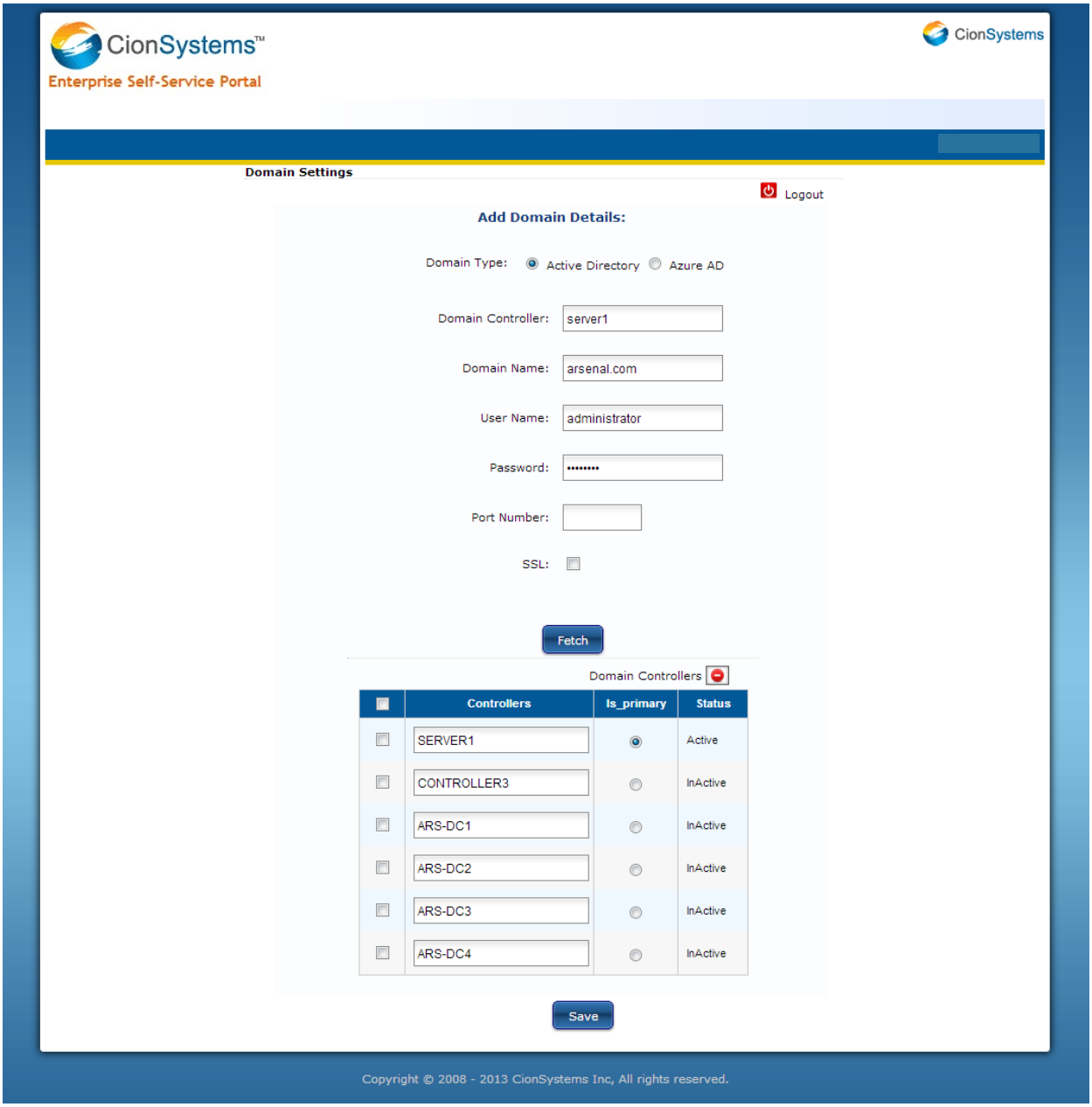
Copyright 2017 CionSystems Inc., All Rights Reserved

The login screen will open in the default web browser. When logging to the application for the first time

- Enter "admin" in the User Name dialogue box.
- Enter "admin" in the Password dialogue box.

❖ **Note: It is recommended that the user name and password should be changed after the application has launched.**

Copyright 2017 CionSystems Inc., All Rights Reserved



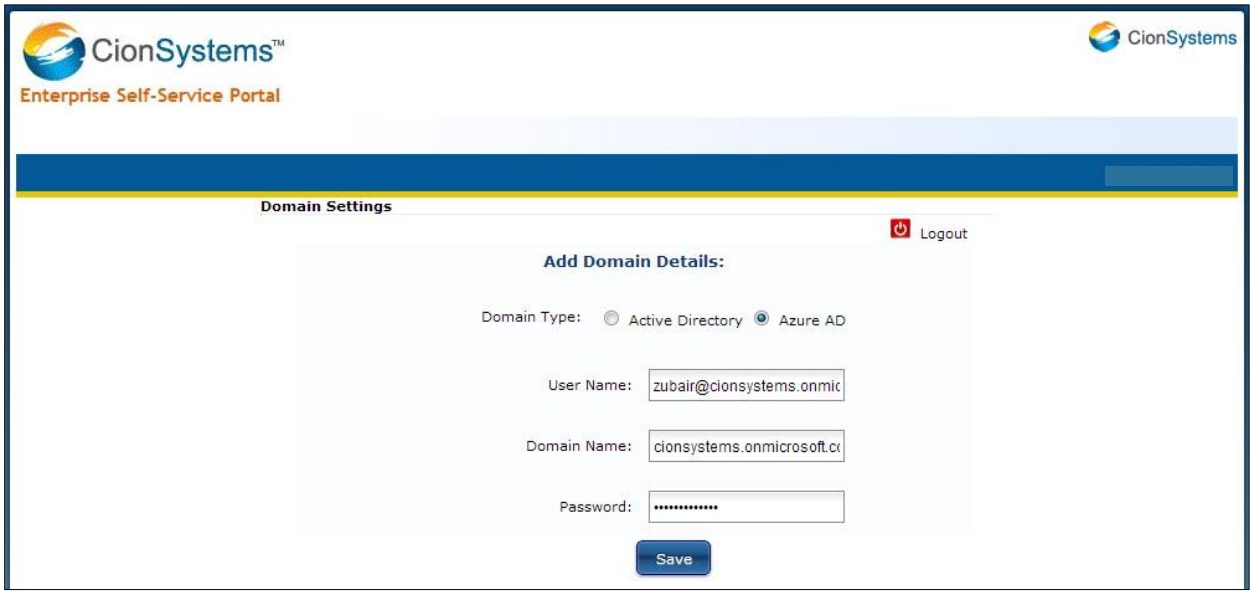
Active Directory

3. Enter the Active Directory Self Service details of the domain.

- Domain Controller.
- Domain Name
- Domain User Name.
- Domain Password.
- Click on the hour glass to choose an OU
- Click on fetch to bring all domain controllers

Copyright 2017 CionSystems Inc., All Rights Reserved

- Select Primary Radio Button
- Click on Save



Azure AD

Note: If you modify an existing backend user name and password for a domain than you must restart IIS service.

To restart IIS service,

→ Click on start,
→ Click on run
→ Type IIS reset command.

Q: How does the registration process works?

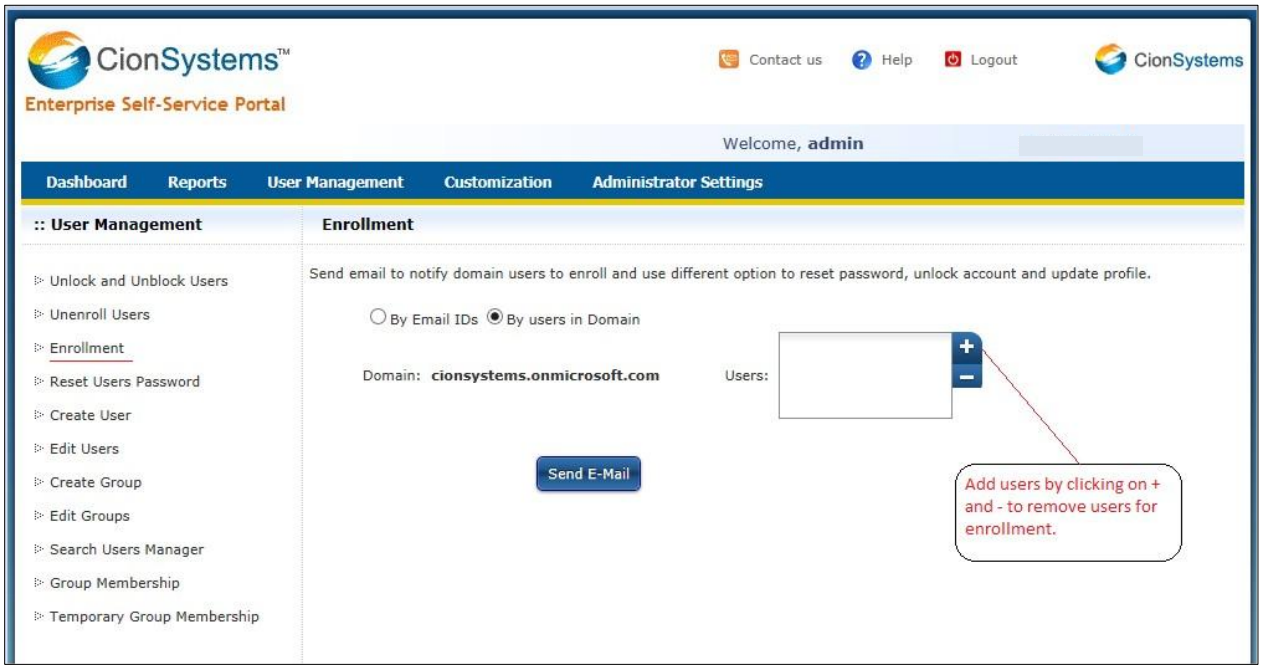
A: Administrator has to create user accounts. There are two options for registering users.

Option1:

After creating user, administrator sends an email to user with enrollment URL using enrollment option. By clicking on enrollment URL, users have to enter his/her username (for AZURE AD), User name and password (for AD) in Enterprise Self-Service portal. Another email is sent for registration, with registration URL. By clicking on Registration URL, User is redirected to Enterprise Self-Service Portal registration page. Here user will select the answers to security challenge questions

Copyright 2017 CionSystems Inc., All Rights Reserved

and edit few personal details. Only registered users with the portal are allowed to reset their password, lock/unlock accounts, modify profile, modify challenge answers etc.



Option2:

After creating user, administrator should notify user by sending user login page URL through email. In user log in page, click on new user registration option and register.

Q: How does "Account Unlock" option work?

A: It works similar to password reset. The user is asked to provide answers to the security questions before their account is unlocked. Note, if LDAP is set to "auto unlock" then the accounts will be automatically unlocked. Additionally, in the application admin can set auto unlock feature so that accounts are unlocked after certain period.

Q: What happens if certain user doesn't register?

A: Only registered users will be able to reset their password and unlock their accounts.

Q: How do I find out which users are registered with the application?

Copyright 2017 CionSystems Inc., All Rights Reserved

A: From admin page

- Click on "User Management Tab"
- Select the UN enroll option to see a list of all enrolled users.

Administrator

Q: I just installed the self-service application. What options I must configure?

A: Login to Self-Service via admin page. The first step is to configure the domain (see the general section of the FAQ). Once the domain is configured

- Click on 'customization' tab. There are several options that you can configure as per your needs.

Challenge Questions – On this page, you can define and add your own security challenge questions, select the number of questions user must answer and in what order, complexity of answers and how many retry they get before the account is locked.

Email notifications – Via this option you can enable/disable email notifications for the user. Please note that you must configure SMTP server by going to "Administrator" tab, SMS and SMTP settings. Without this configuration, the user creation workflow will not work correctly.

Email templates – You can customize emails that are sent out to the administrators and user community

User policy – You must configure the user policy for it to correctly work as per your need. A selected check box means the user will be able to see and perform that functionality. For example, if you unselect "self-update", then users upon login to the portal will not be able to see and change their user profile.

User profile update settings – If you like user community to modify their own profile then you must select the 'attributes' that you would like them to modify.

Other – You can further customize the portal to your need. You can define the virtual path so that you can direct the internet coming users to connect the application path. Additional, you can enable or disable "two" factor authentication. Note: we don't recommend enabling "enable forgot credential and challenge questions", as this will allow users to reset their credential and answers to security challenge questions via a workflow.

Copyright 2017 CionSystems Inc., All Rights Reserved

Q: How to configure "Reset approval policy"?

A: A policy can be created by following steps

→Login to application with Administrator credentials
→Click on Customization tab
→ Navigate to reset approval policy

- Configuring On Group Policy

  Note: We can create only one policy for a group

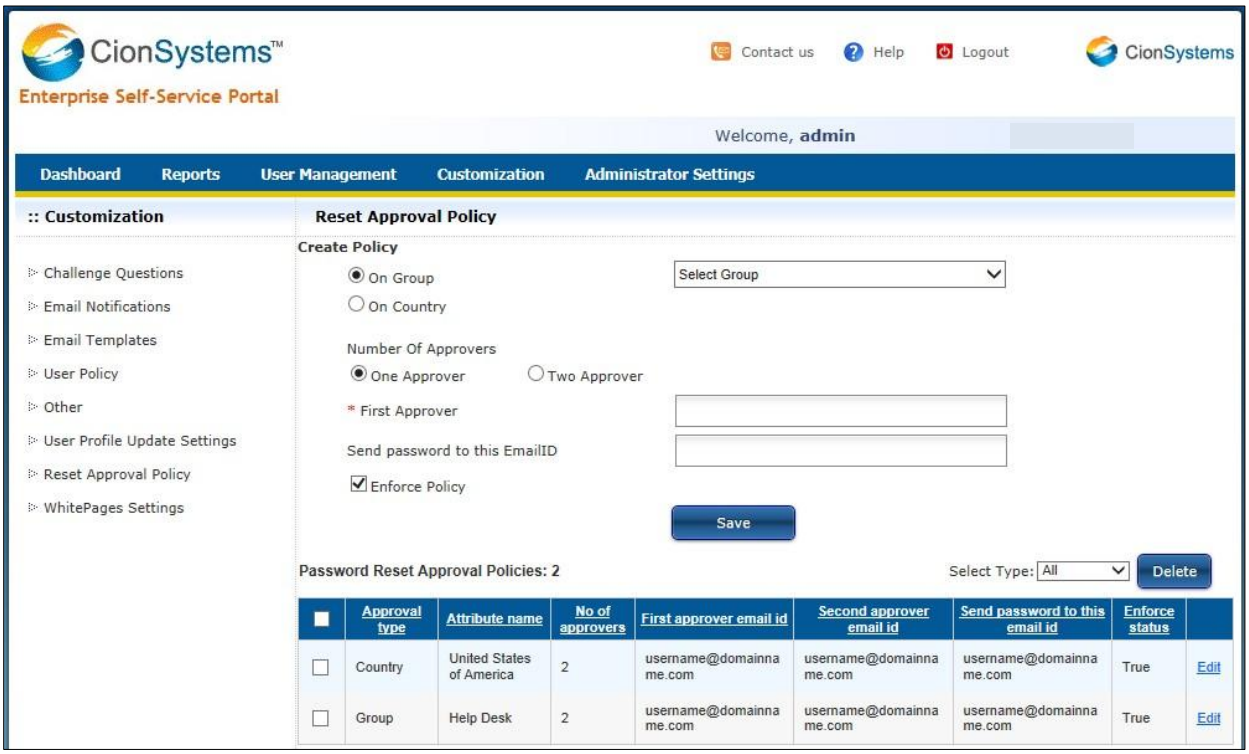
  → Enable On Group
  → Select the required group
  → Enter one approver mail id
  → Enter two approver mail id (optional)
  → Give mail id at "Send password to this Email id"
  → Enable Enforce policy

- Configuring On Country Policy

  Note: We can create many Policies for On country

  → Enable On country
  → Select the required country
  → Enter one approver mail id
  → Enter two approver Mail id (optional)
  → Enter mail id to which password to be sent "Send Password to this mail id"
  → Enable Enforce Policy

Copyright 2017 CionSystems Inc., All Rights Reserved



When administrator reset required user password, an email is sent to approver one and approver two (optional).

After the 'Approvers' approves the Password Reset Request, password will be emailed to the configured email ID and as well as user email ID.

Note: From application we can define policy only for one group. For countries we can define for each country.

When admin resets the password of a user that belongs to both Country and Group, Password Reset Request will be sent to only group approvers. If an approver is assigned for 'All' under countries, whenever the admin resets the password of a user that belongs to any country then the Password Reset Request will be sent to this approver. If the approver is not assigned then the request will be sent to the specific approver for the country. When admin resets the password of a user that belongs to a country for which no approvers are assigned, password will be reset directly. If this option is not defined password will be mailed to User ManagerCionSystems Inc. Copyright 2013

If approver approves the request, the password will be emailed to Email ID defined in 'Send password to this Email ID'.CionSystems Inc. Copyright 2013

Copyright 2017 CionSystems Inc., All Rights Reserved

When admin Resets Password of User who doesn't belong to any group or Country defined in Approval Policy, their password will be Reset immediately (without invoking approval process) and password will be mailed to his/her (User) Manager.

Q: What is in Administrator settings tab?

A: This section allows you to do many administrative type of task. Here is a list of options

Domain settings – From this section you can modify the existing domain configuration including the service account and credential, OU for the user creation, domain controllers. Additionally, you can switch between AD and openLDAP configuration. Performing a domain switch will cause some of the user data, application configuration data to change.

SMTP and SMS settings – In this section you can configure the SMTP settings for receiving and sending emails. Self-service portal supports both on premise SMTP server or cloud based SMTP server like office365, Google mail etc. SMTP configuration is required for the application correctly. Additionally, you must configure the administrator email address. SMS setting is optional. Self-service portal supports SMS as the second factor. In order to use SMS, make sure you have signed up with SMS gateway service and have the required configuration available.

Add your company logo – You can add your company's logo to the self-service portal.

Change password – You can change the administrative password to your desired password. Note, write down the password some place secure. Application encrypts and stores the password.

Register IP address for authentication service – Self-service exposes programming interfaces for any web applications to leverage the authentication engine, user self-service and user password registration management. Application provides highest security by encrypting the data flown from the calling application to authentication service; additionally it honors only calls from the registered IP addresses.

Q: What is user management?

A: Here administrator can perform day to day operations such as administrator trigger password reset.

Unlock Unblock users – Administrator can unlock users from domain and also unblock users from using the portal. Block happens when user enters incorrect security questions.

Copyright 2017 CionSystems Inc., All Rights Reserved

UN Enroll users – Here administrator can see all users that are not registered with the portal. Administrator can disable/delete those users from the domain.

User's password reset – Administrator can "reset" the user password. A random password is generated and sent to the user email ID. The administrator will not know the user password.

Delete users – Administrator can delete users from the domain. Select edit user option and search for required users and select them and delete.

Q: What is the report section?

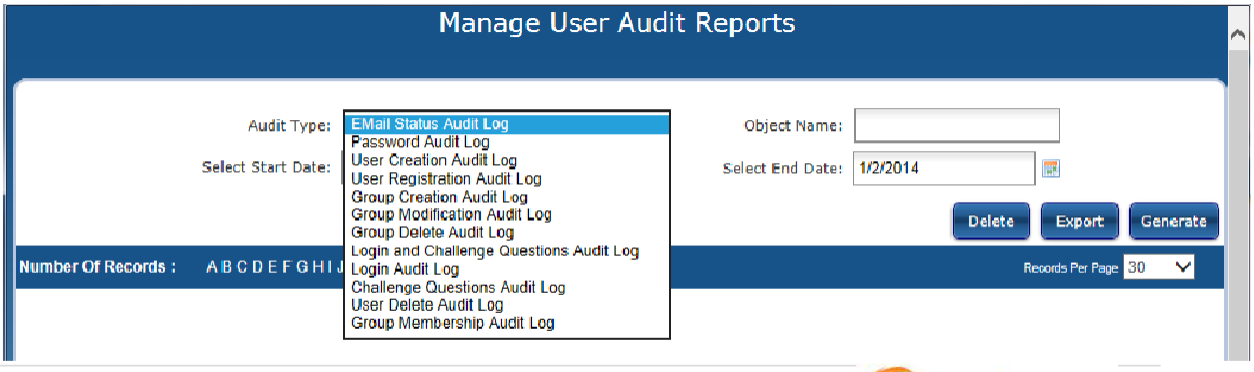
A: Self-service provides two types of report. Basic domain reports and audit trail report from the portal activity. It tracks all user activities an administrator can generate time period activity report for the application including logon reports.

User reports – Under this section you will see

- All user reports
- Soon to expire password report
- Locked out users
- Password expired users
- Enrolled users
- Not enrolled users
- User events

Audit reports – Under this section you can generate user audit trail reports

- Reset Password Audit Report
- Un Locked Users Audit Report
- User Update Audit Report
- Manage User Audit Reports
- Email Status Report
- Failed Attempts at Challenge Questions by users
- Reset Challenge Question Answers Report



 Copyright 2017 CionSystems Inc., All Rights Reserved

Users

Q: How to assign a manger for a user in Office 365/ Azure AD?

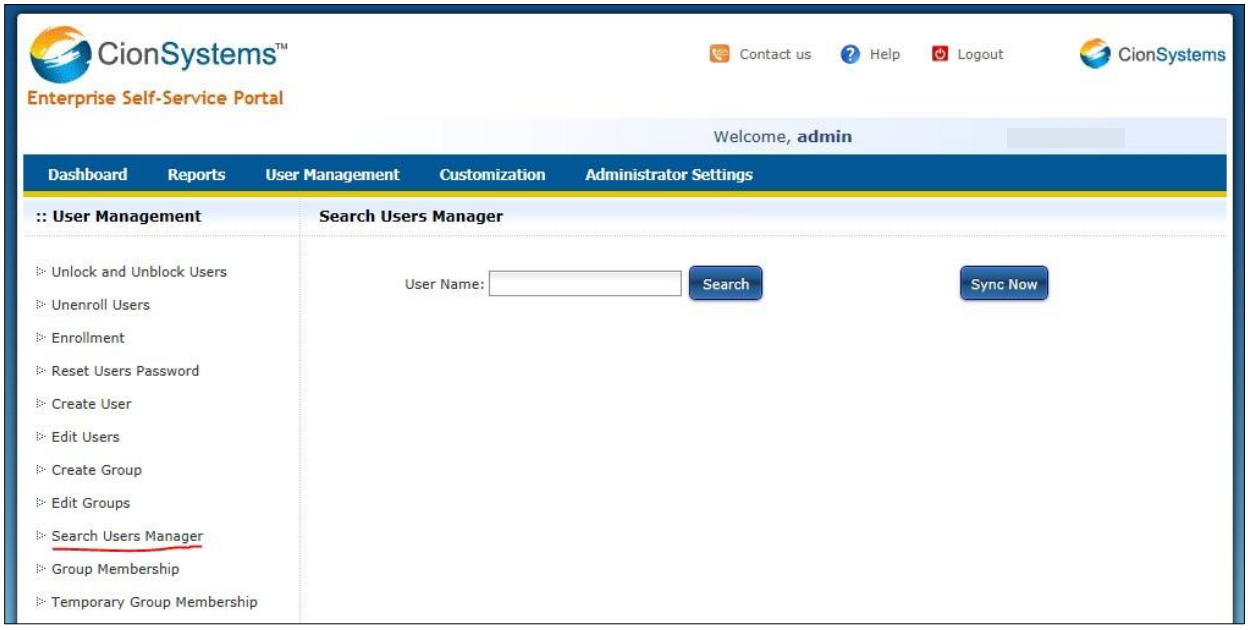
A: Admin can assign a manager for a user by following steps

→ Log in to administrator Portal
→ Navigate to user management
→ Edit user-search
→ Select user
→ Assign manager while editing user profile

Q: How to search for User's Manager?

A: Search for User's Manager

→ Log in to admin portal
→ Click on User Management
→ Navigate to Search user's manager
→ In search box enter required user name and search



Q: How does a user log in to the Enterprise Self-Service application? (AD & Azure AD)

Copyright 2017 CionSystems Inc., All Rights Reserved

A: A user can login to the Enterprise Self-Service application by following the below steps. *Please see the general section for user URL*.

- → Click on Internet Explorer, Chrome, Firefox or safari
- → Type the administrator provided URL for Enterprise Self-Service Application
- → Choose the activity
- → For login
  - ✓ Provide their username
  - ✓ Credentials
  - ✓ Click on "Login" button.

After the validation of credentials the user will see their profile settings.

Note: If two factor authentication is enabled than the application will ask security challenge questions.

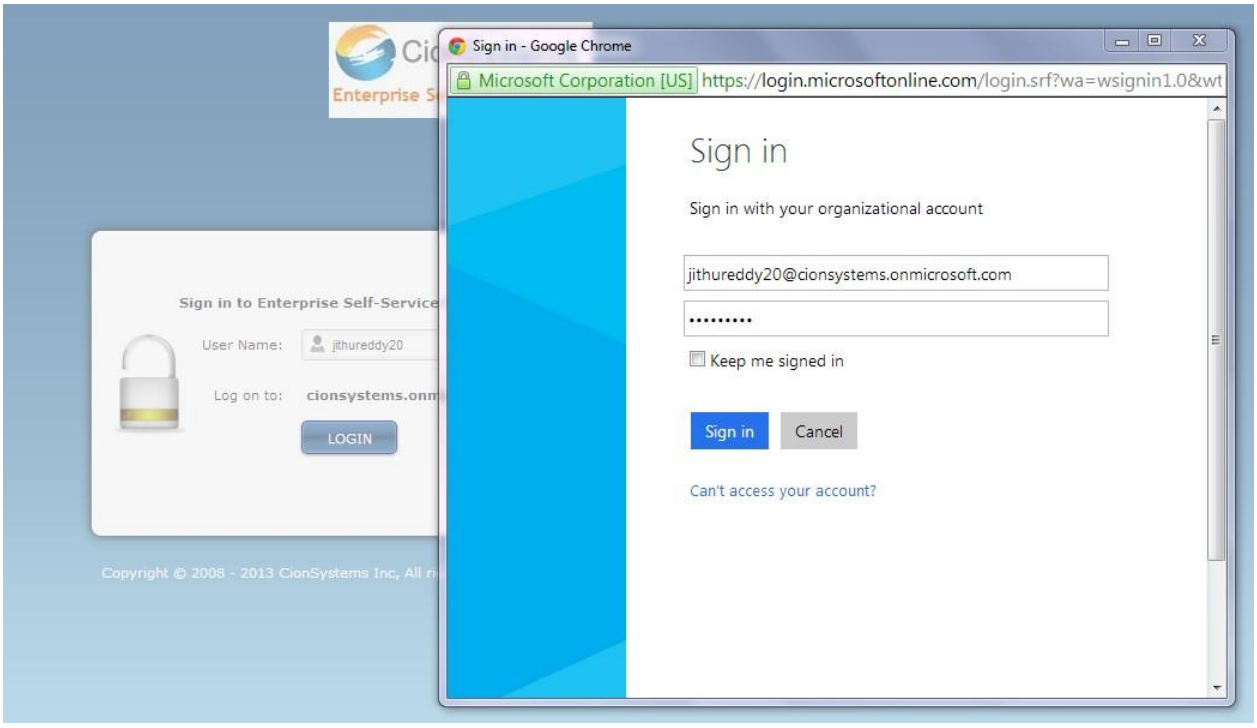
User log in AD mode

Copyright 2017 CionSystems Inc., All Rights Reserved

Q: How does Office 365 user log in to self-service?

A: Open any browser and enter URL provided for user

→ Enter User name
→ Click on'login'
→ A new window will pop up from Microsoft web site with login page
→ Enter user name, enter password
→ Click on Sign in
→ Enter Challenging question's answers
→ Now application will allow user to log in.



User Log in Azure AD

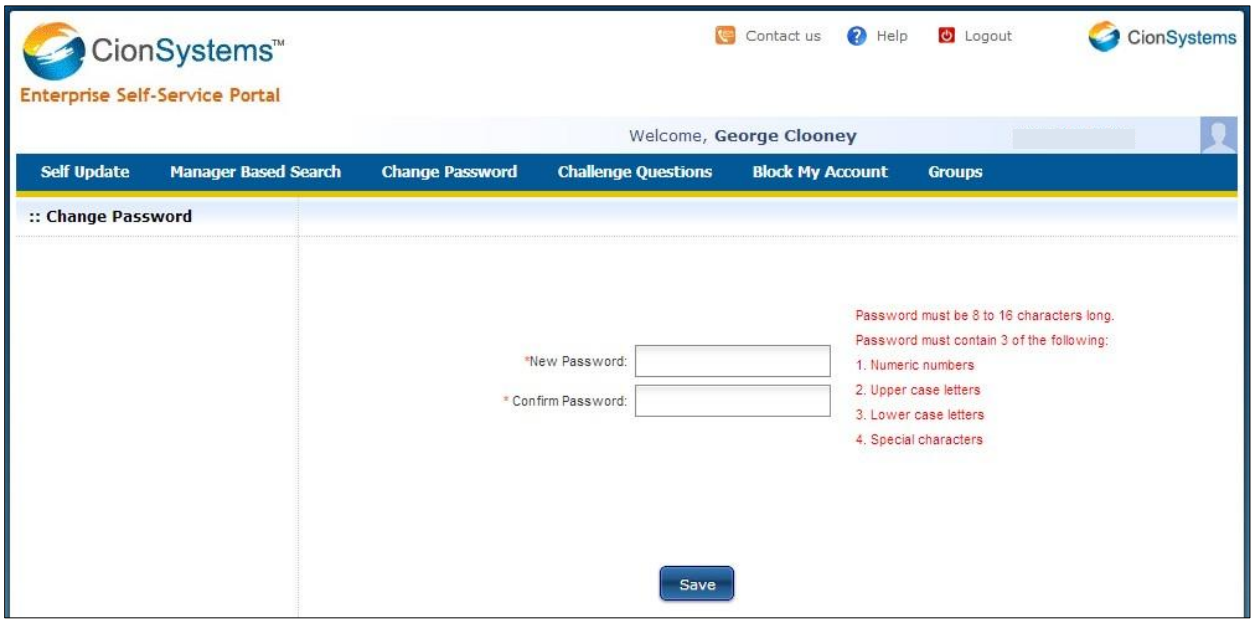
Q: How do users change their passwords?

A: User have to login to the application using their domain user credentials and follow the below steps

- Click on "Change Password" tab

Copyright 2017 CionSystems Inc., All Rights Reserved

- Enter New Password and Confirm Password
- Click on the "Save" button



Q: Users can't see some of the settings in their profile when they login to Enterprise Self-Service application. What could be wrong?

A: Most likely the administrator has removed access to these attributes for Enterprise Self-Service.

Q: When a user tries to update settings, they receive "access denied error", what could be wrong?

A: The most likely reason is the backend connection to LDAP doesn't have sufficient privileges to affect the change. Administrators must ensure the Enterprise Self-Service application is configured to connect to the domain with a domain administrative level account.

Q. How do I configure Office365?

Self-service supports Microsoft Active Directory and Azure AD. You can't configure AD and Azure AD at the same time. If you need then you will need separate install one for each.

Copyright 2017 CionSystems Inc., All Rights Reserved

To *Configure a Domain*

- Click on Start Button>All Programs> Enterprise Self Service> Enterprise Self Service icon.

OR

Click Enterprise Self Service Icon on desktop and follow the below procedure

The login screen will open in the default web browser. When logging to the application for the first time

- Enter "admin" in the User Name dialogue box.
- Enter "admin" in the Password dialogue box.

Enter the Azure AD details.

- Enter User Name.
- Enter Password and Click on Save Button

Power Users

Q: How does a Power user log in to the Enterprise Self-Service application?

A. A Power user can login to the Enterprise Self-Service application by following the below steps

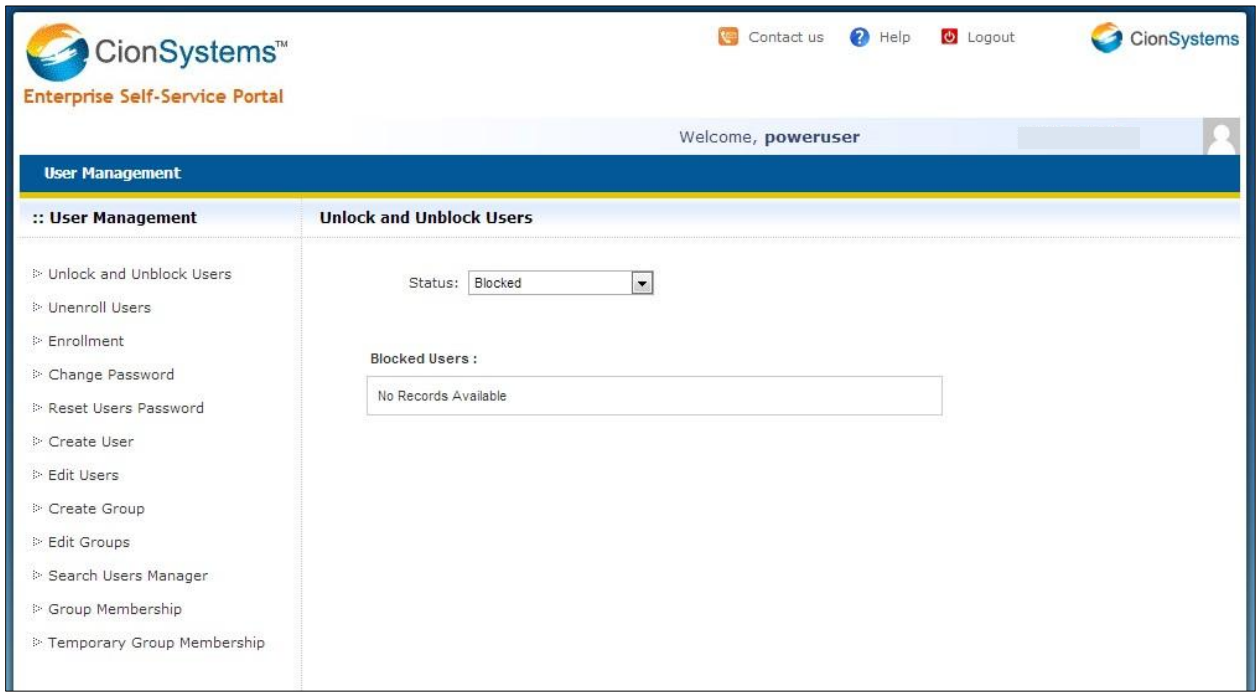
Add Domain to Application

Click Enterprise Self Service Icon on desktop and follow the below procedure.

Copyright 2017 CionSystems Inc., All Rights Reserved

- Enter "power user" in the User Name dialogue box.
- Enter "user" in the Password dialogue box

Copyright 2017 CionSystems Inc., All Rights Reserved



Power user

Power user can perform the below operations

- Unblock and Unlock Users
- Un enroll Users
- Users Password Reset
- Edit Users
- Create User

Q. How do I configure Primary IT manager and Secondary IT manager for Password Approval?

A. Login to Enterprise Self-Service via admin page

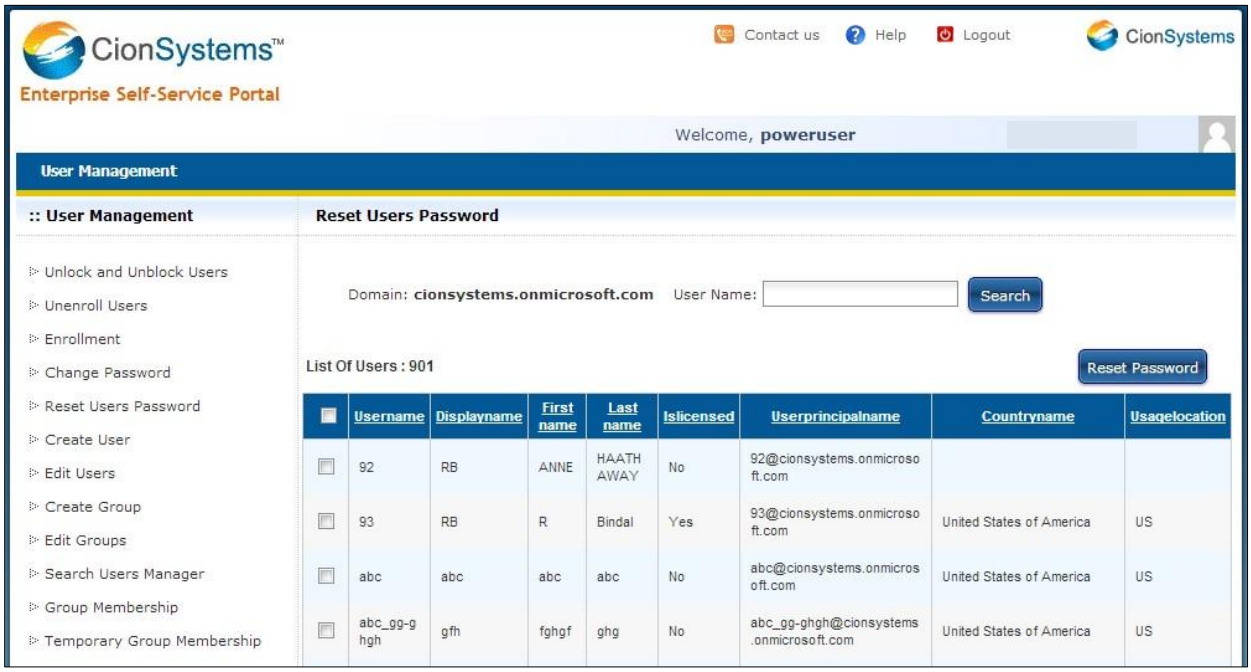
- Click on 'customization' tab
- Click on Reset Approval Policy
- Configure Primary manager(Approver1) and Secondary manager(Approver2) email id's

Copyright 2017 CionSystems Inc., All Rights Reserved

Q: How does an admin or Power user Reset Users password?

A. Login to Self-Service via admin page with admin or power user credentials

- Click on User Management
- Click on Users Password Reset
- Click on Search



→ Select Users and click on Reset Password

→ After Managers Approval password will be Reset

→ If the user is configured for reset approval policy, then reset approval policy work flow is implemented.

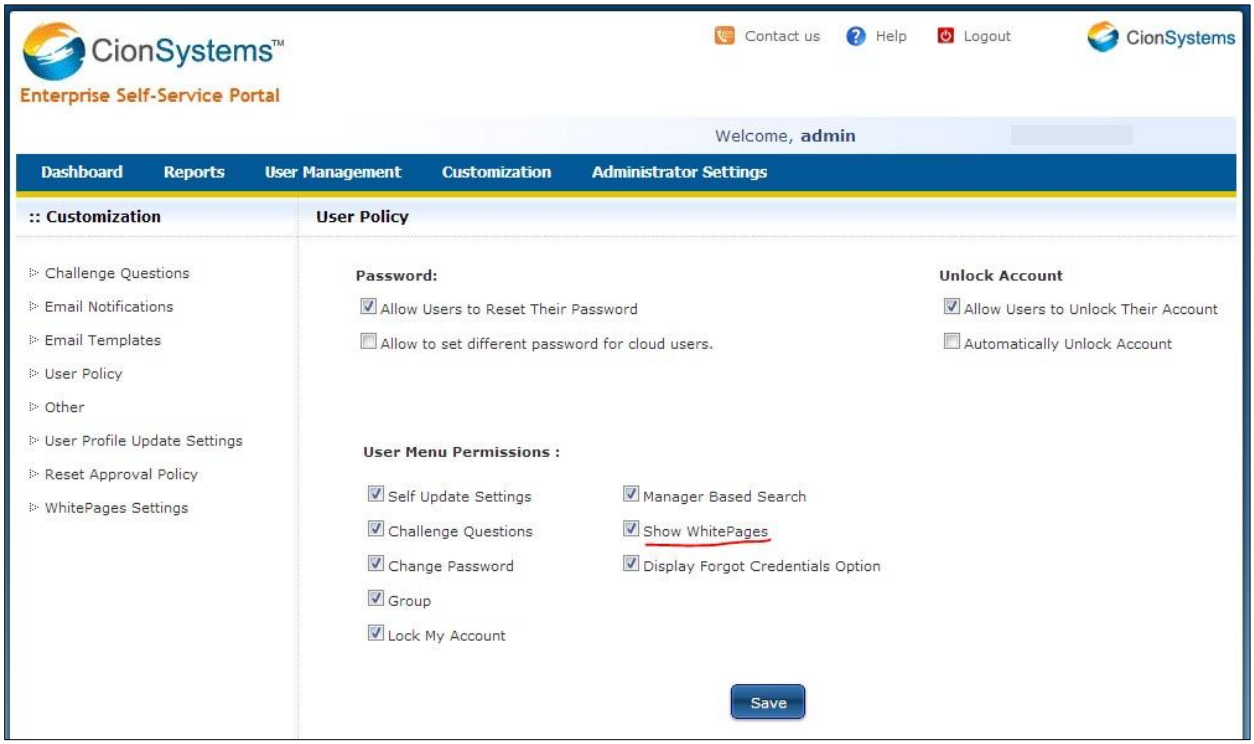
→ If user is not configured with reset approval policy, then password is directly reset.

Copyright 2017 CionSystems Inc., All Rights Reserved

Q: How do I configure white pages?

A: Follow the steps to configure white pages in user login page.

→ Login to Admin Profile
→ Go to customization tab
→ Click on User Policy
→ Enable show white pages option.



Q: How do I search users without log in to application?

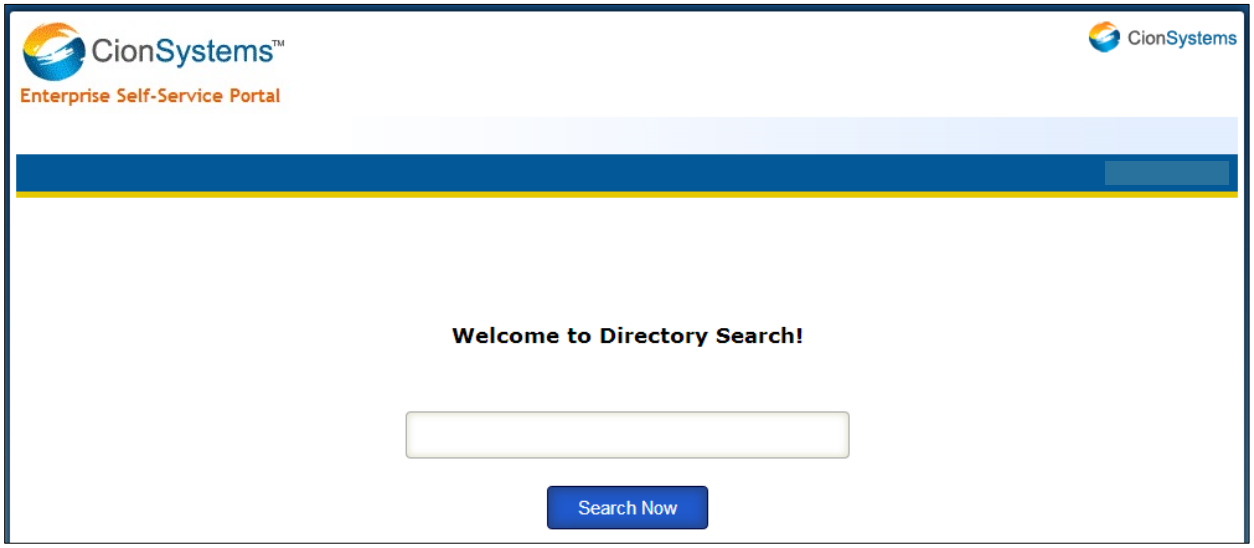
A: By using white pages you can search for any user. Here you can see details for any user.

Follow the steps to search and see (Read only) the user profile.

→ Open application user log in page
→ Click on white pages
→ A new tab is opened in your browser
→ Type the required user name or first name or last name

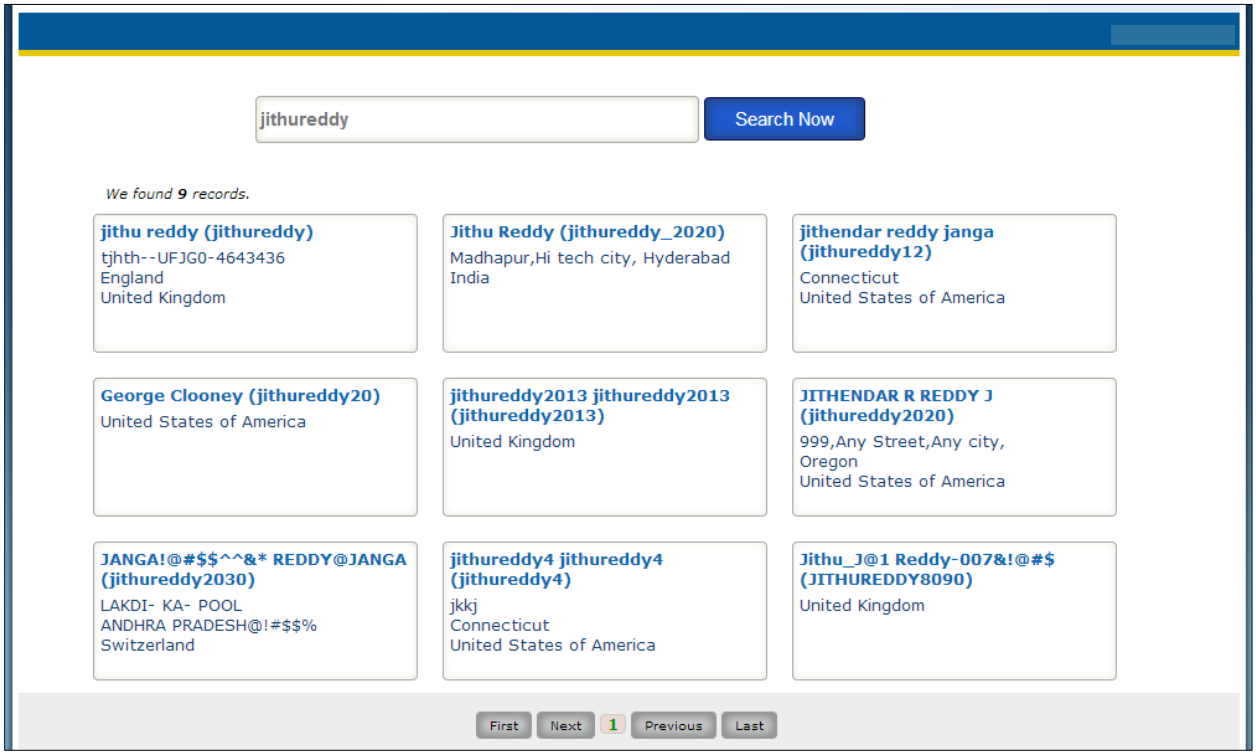
Copyright 2017 CionSystems Inc., All Rights Reserved

→ White pages will display all users with similar string searched for.
→ Click on required user.



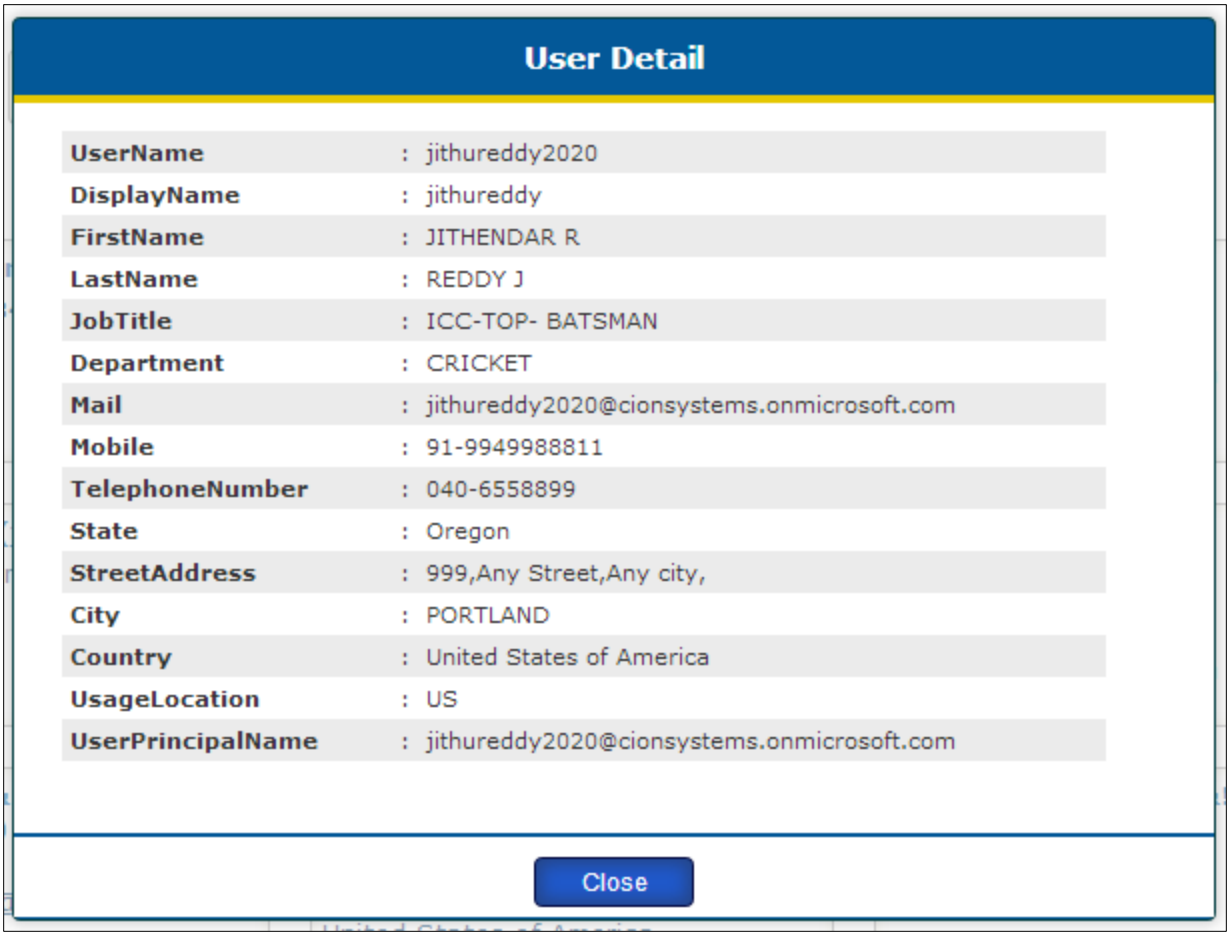
Copyright 2017 CionSystems Inc., All Rights Reserved

Enter the required user details like User name, First name or last name.



If we click on user, all his details are displayed in a pop up.

Copyright 2017 CionSystems Inc., All Rights Reserved



NOTE: All the above details shown in white pages are 'Read only'.

Copyright 2017 CionSystems Inc., All Rights Reserved