Universal Cloud Portal Sign-In Guide

- In Universal Cloud Portal login screen - Enter registered email and password and display Captcha and click on Login to Sign-In to Portal.
  If user not yet to reset the password then user will navigate to reset password screen once after validating with current password to reset password with new password policy to increase more security to account.

- In case if user not yet reset the password with new password policy then user will navigate to below screen to reset password and it is mandatory to reset for security purpose.
  Random Password Generator option is also available to generate suggested password with valid new password policy, below are the highlight terms of password policy:
    o Password must contain min 14 characters and max 32 characters
    o Password must contain atleast 3 alphabet characters
    o Password must contain atleast one Small & Capital letter and one Number & one special character
    o Space and . , ( ) % These Special characters are not allowed in Password
    o Password must not contain more than 2 sequential repeated characters. *eg: sm**aaaa**rr**tttt**, universal**llll***
    o Password must not contain more than 2 sequential numbers and reverse numbers. *eg: smart**123456**, smart**654321***
    o Password must not contain more than 2 sequential alphabets and reverse alphabets. *eg: smart**abcdef**, smartfe**dcba***
    o Password must not contain any common words like **cloud4c, c4c, ctrls, ucp, myshift, welcome, password, admin** *and* **user name/mobile number** and must not contain reverse of any common words also
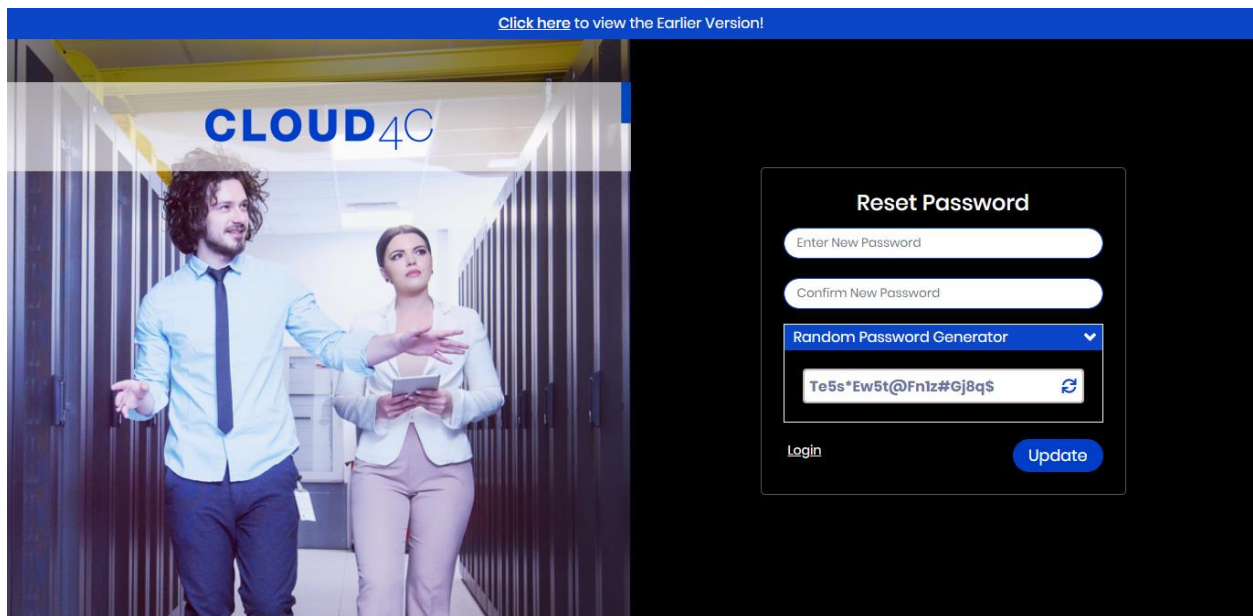
- This step need to do only once while log in into the portal for the first time after this feature introduced, User need to enter Secret Key by scanning QR Code in Google Authenticator mobile App to login for more security, for more details follow below steps
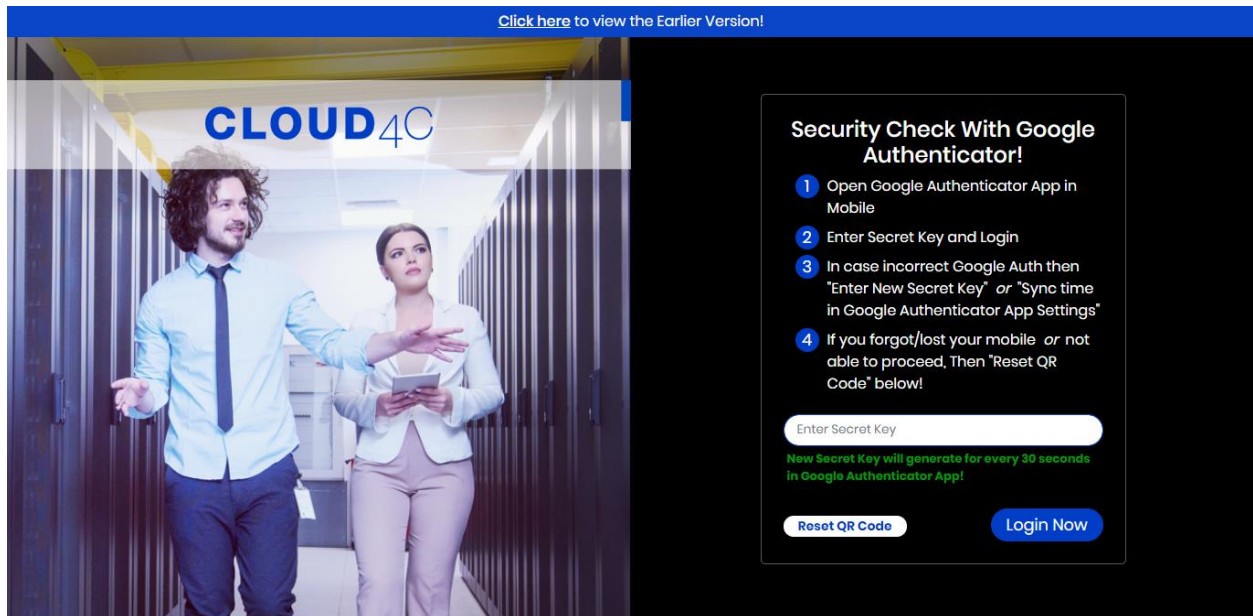 - o Download Google Authenticator App in Mobile
  - o Sync time in Google Authenticator App Settings
 - o Scan displayed QR Code
  - o Enter Secret Key and Login

- User need to check Secret Key in Google Authenticator Mobile App and enter Secret Key to login from second time of registering QR Code, for more details follow below steps
  - Open Google Authenticator App in Mobile
  - Enter Secret Key and Login
  - In case incorrect Google Authorization then "Enter New Secret Key" *or* "Sync time in Google Authenticator App Settings "
  - If you forgot/lost your mobile *or* not able to proceed, then click on "Reset QR Code" to generate new QR Code

- OTP will send to Registered Email and Mobile automatically when redirects here.
  Enter OTP and Reset QR Code then it will navigate to Security Check with Google Authenticator screen and Scan QR Code in Google Authenticator App and enter Secret Key to Login!
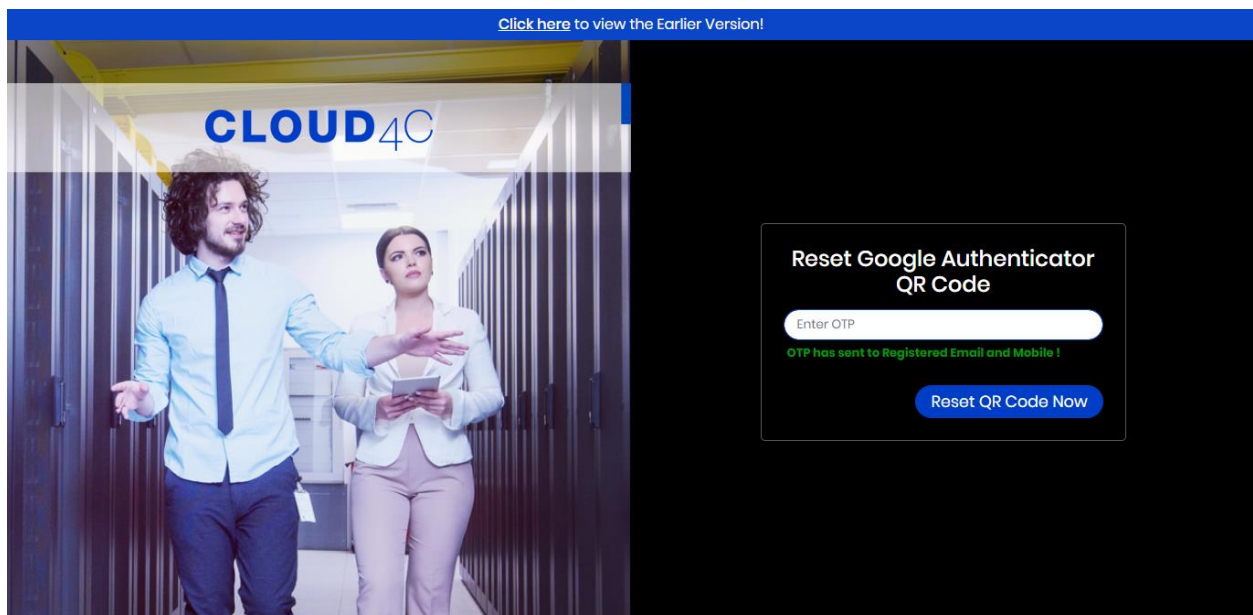
- In case Forgot Password then click on Forgot Password link in login screen and it will navigate to here. Enter registered email then Reset password link will send to registered mail id.