



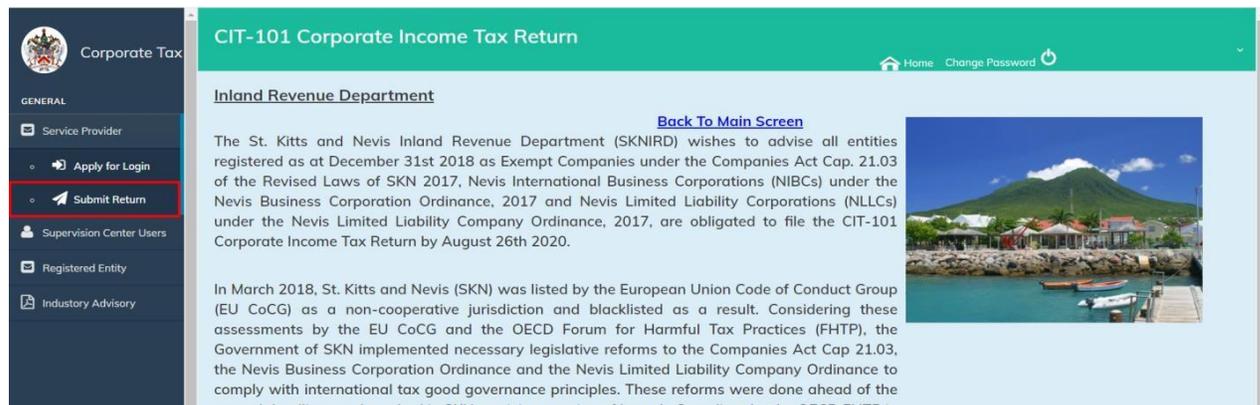
## **USER GUIDE FOR 2FA Authentication Setup**

## 1. Introduction

The CIT-101 User Manual is designed to guide users through the implementation of Two-Factor Authentication (2FA). This Document provides step-by-step instructions on how to enhance system security with 2FA and effectively manage user sessions.

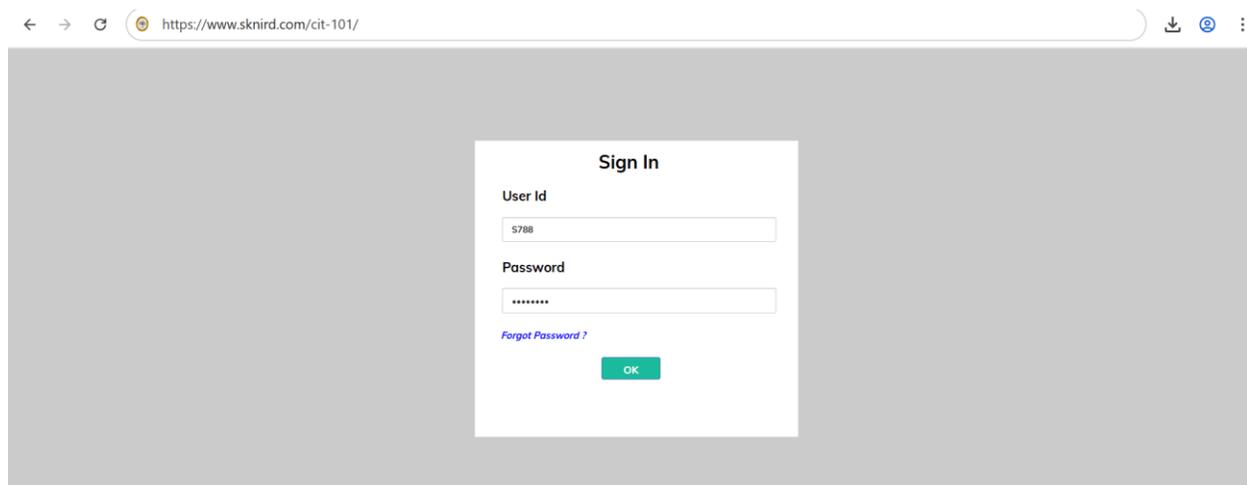
## 2. How to access the application

The user can access the web application by using the <https://www.sknird.com/cit-101/>. After that, he needs to click on the "Submit Return" link, which is located under the "Service Provider" section in the application.



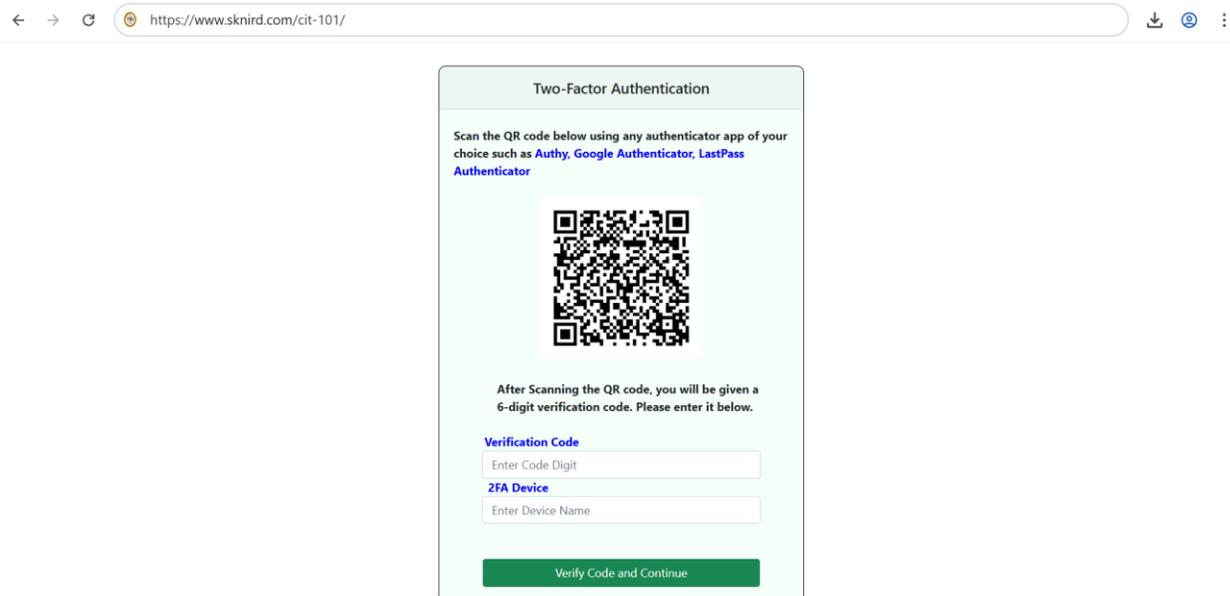
## 3. Login Screen.

By clicking on the "Submit Return" user will be able to see the login screen over there he has to provide the valid credentials for login (e.g., User ID: 'S788' and Password: 'Test@123')



## 4. 2FA Registration Functionality:

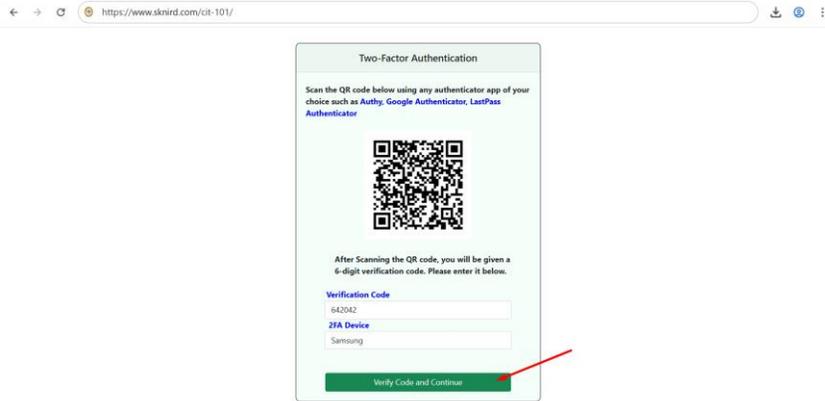
- After a successful login, the user is redirected to the **2FA Registration** page.
- On this page, the user is prompted to **scan a QR Code** using a recommended authenticator app (e.g., Google Authenticator, Microsoft Authenticator, Authy).



- The QR code is generated using a **unique user-specific key**, and it includes:
  - **Issuer:** CIT
  - **Account:** The user's ID (e.g., **S788**)
  - This ensures the authenticator app displays the label in the format: **CIT : S788**, making it easy to identify the user when managing multiple codes.



- Enter the **6-digit** verification code generated by the app (no extra spaces, only a 6-digit code without any spaces).
- **Provide the device name** for identification purposes (e.g., **SAMSUNG**).

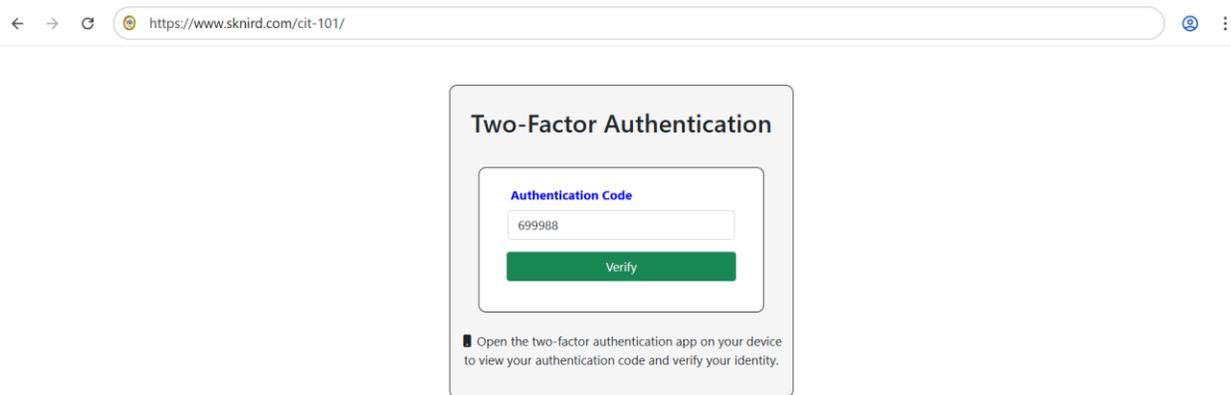


- Click "**Verify Code and Continue**" to complete the 2FA registration.
- If the verification is successful:
  - The user's **PASS\_KEY** and **2FA\_Device** are securely stored in the Database.
  - The user is granted access to the secure area of the system.

After clicking on 'Verify and Continue', if all validations are successful, the user will be redirected to their dashboard or main application page.

Application ID	Filing Year	Application Status	Fiscal Year Start	Fiscal Year End	Tax Payer No	Company Registration No	Corporation Name	Edit	Delete	New	Print
43040	2023	SUBMITTED	01/01/2023	31/12/2023		56782	TestLogix.com	Edit	Delete	New	

- Once the user has registered for 2FA, they will be redirected to the 2FA Verification OTP page upon logging in again after logging out.
- If 2FA is already set up:
  - The QR code and verification form are hidden, and only the verification screen is shown.
  - At this stage, the user must enter the six-digit OTP generated by the authenticator app they set up earlier (no extra spaces, only a 6-digit code without any spaces).



After verifying their OTP by clicking the **Verify** button, the user is redirected to their dashboard

