Identity and Access Management

Multi-Factor Authentication (MFA)

End-User Guide

Table of Contents

Tel 800342 | P.O. Box 4545 Dubai, UAE | dha.gov.ae | info@dha.gov.ae | ص.ب. 4545 دبي إ ع م | هاتف 800 342

Tel 800342 | P.O. Box 4545 Dubai, UAE | dha.gov.ae | info@dha.gov.ae | ص.ب. 4545 دبي إ ع م | هاتف 800 342

1. Introduction

This document provides a detailed step-by-step explanation of the Multi-Factor Authentication (MFA) process implemented for Dubai Health Authority (DHA) portal users. The purpose of MFA is to enhance account security by requiring additional identity verification beyond a username and password.

1.1 Document Purpose

This guide explains:

- MFA enrolment during registration
- MFA verification during login
- Email and mobile verification for existing users
- Password reset using MFA
- Username recovery processes

1.2 Overview of MFA Process

The MFA process includes the following components:

- Email verification using a One-Time Password (OTP)
- Mobile number validation using an OTP
- OTP-based authentication during login
- Device registration

1.3 General Notes

The following notes should be reviewed before using the system:

- In all forms, (*) indicates a mandatory field.
- OTPs (One-Time Passwords) are time-sensitive and valid only for a limited duration.
- An OTP will be sent to the registered email address or mobile number.
- Do not share your OTP with anyone.
- If an OTP expires, click “Resend Code”.
- Multiple incorrect OTP attempts may temporarily lock the account.
- Email and mobile number verification are mandatory for MFA activation.

2. External User Registration and Authentication Procedures

This section describes the registration and authentication processes applicable to external users accessing the DHA portal.

2.1 New User Registration

This section explains the registration process for external users accessing the DHA portal.

Note:

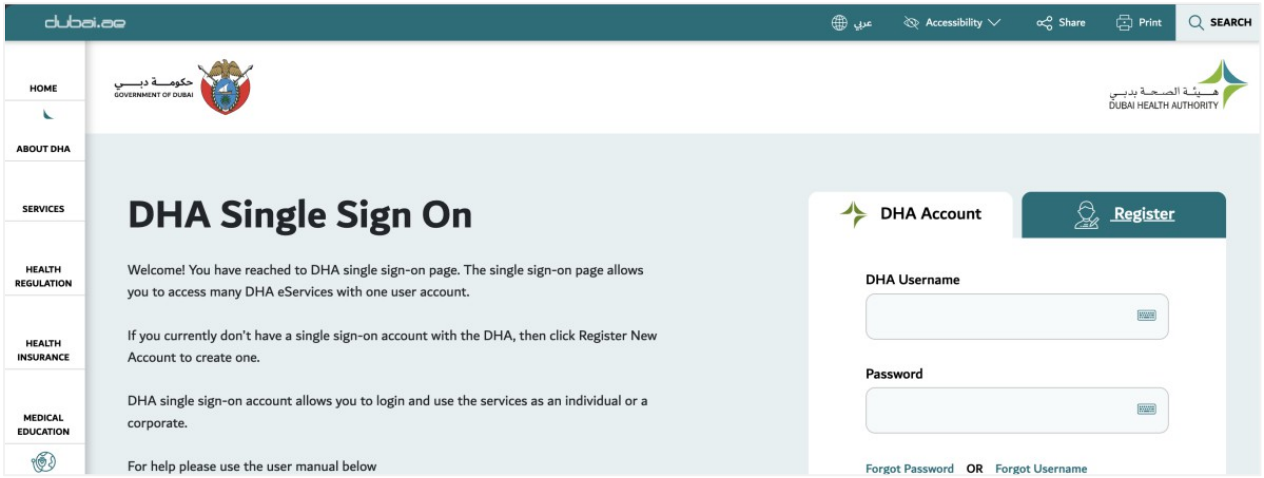
Internal users are provisioned through internal identity management processes and are not required to self-register through the portal.

Step 1: Access the Registration Page

Navigate to the DHA portal login page:

https://services.dha.gov.ae/

Click on the **"Register"** icon



Step 2: Enter Mandatory Registration Details

The user must provide all mandatory information:

- Username (must be unique)
- Email address (mandatory)
- Password
- Confirm password (must match the password entered)
- First name (mandatory)
- Mobile number (mandatory)
- Nationality (mandatory)

The user may also provide additional optional information if required.

Select the checkbox **"I am not a robot"**.

Click on **"Register"**.

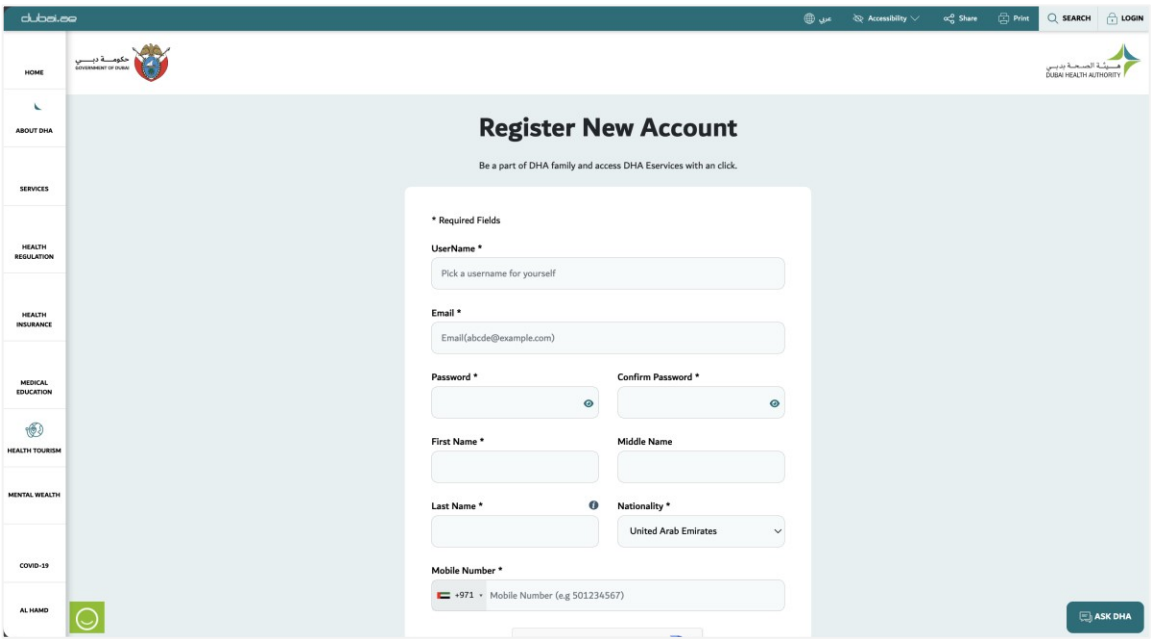


Figure 2.1.1 – Registration Page

Step 3: Email OTP Verification

After clicking "**Register**":

- The system generates a One-Time Password (OTP).
- The OTP is sent to the email address provided during registration.
- The user is redirected to the Email OTP Verification Page.

The User must enter the OTP received in the registered email and click **"Submit".**

Note:

If the OTP is valid, the email address is successfully verified.

If the OTP is invalid or expired, an error message is displayed. The user may retry or click **"Resend Code."**

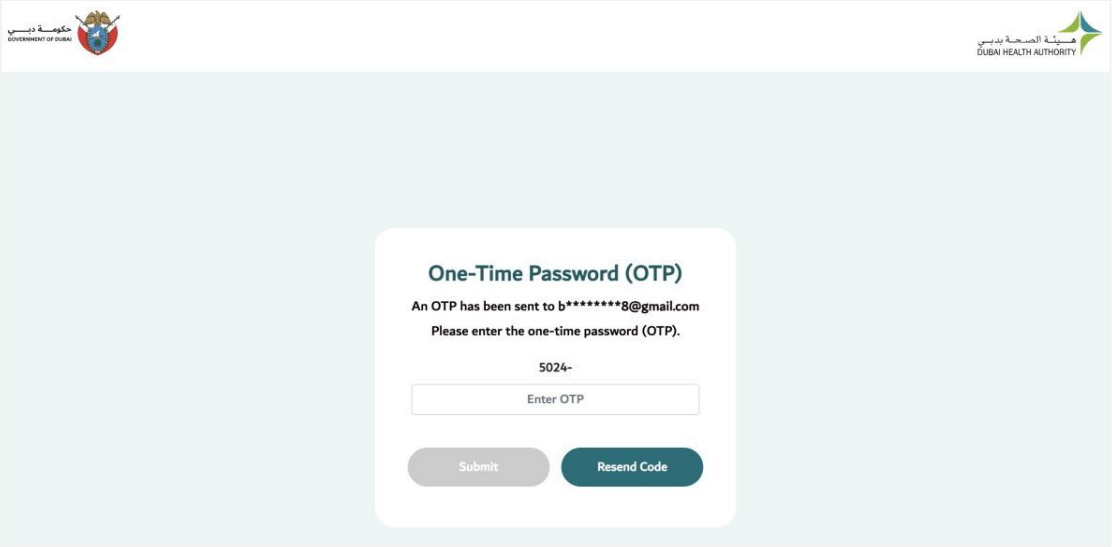


Figure 2.1.2 – Email OTP Verification Screen

Note: at this point user account created in IDAM and Mobile number verification has been started. In case user account creation failed, user will not proceed with mobile number verification step.

Step 4: Mobile Number Validation

After successful email verification, the user is redirected to the Mobile Number Validation Page.

The system displays the masked mobile number entered during registration.

The user may edit the mobile number if required.

Click "**Continue**".

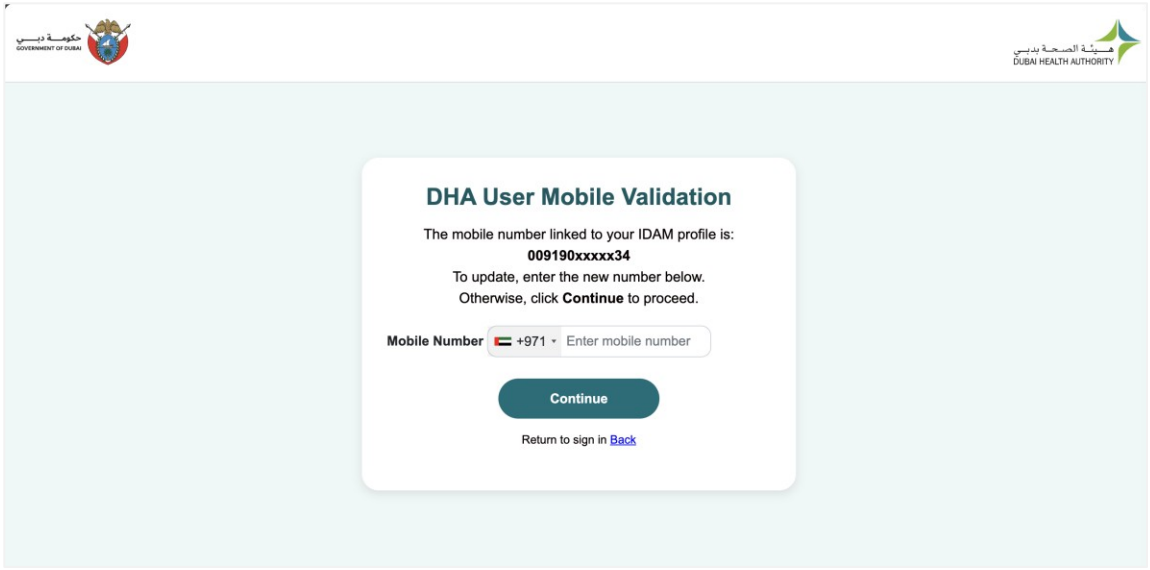


Figure 2.1.3 – Mobile Validation Screen

Step 5: Mobile OTP Verification

After clicking "**Continue**":

- The system generates a One-Time Password (OTP).
- The OTP is sent to the registered mobile number.
- The user is redirected to the Mobile OTP Verification Page.

The User must enter the OTP received via SMS and click "**Submit**".

Note:

If the OTP is valid, the mobile number is successfully verified.

If the OTP is invalid or expired, an error message is displayed. The user may retry or click "**Resend Code**".

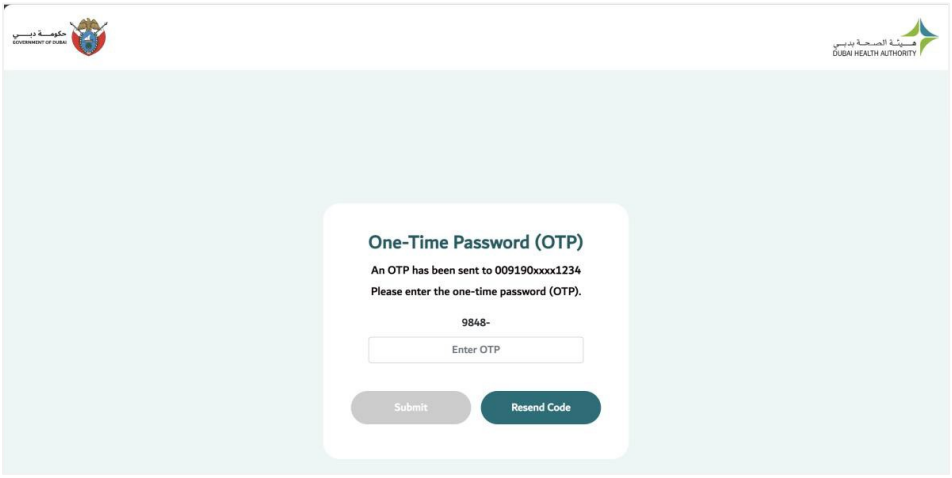


Figure 2.1.4 – Mobile OTP Verification Screen

Once both verifications are completed, the registration process is finalised. The user account is activated and the user can proceed to log in using their registered username and password.

Figure 2.1.5– Application Screen after Log

2.2 Existing User Login – Verified Email and Mobile

This section explains the login process for existing users whose email address and mobile number are already verified.

Step 1: Access the Application Login Page

Navigate to the DHA portal login page:

https://services.dha.gov.ae/

Enter the credentials: username and password.

Click on **"Login"**.

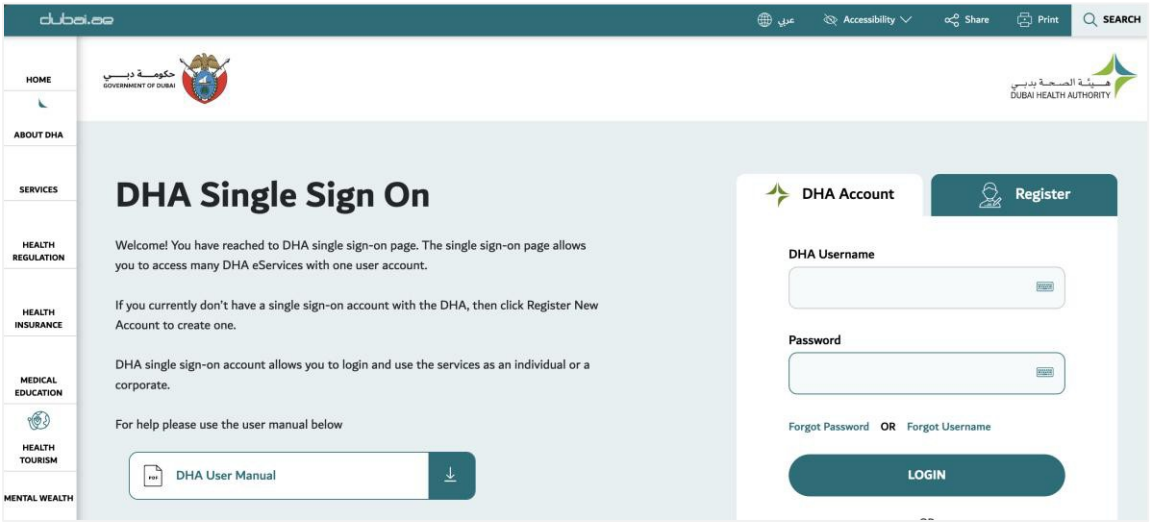


Figure 2.2.1 – Login Screen

Step 2: Multi-Factor Authentication Method Selection

After successful validation of the username and password, the system displays the **MFA Authentication Method Selection Page.**

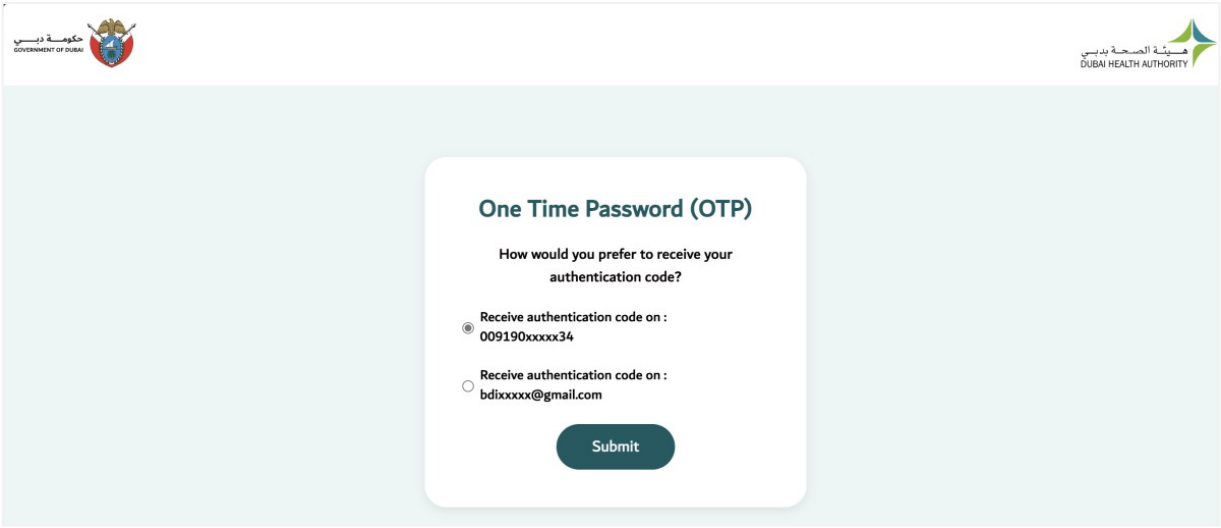
The user must select one of the available authentication methods.

For external users:

- Receive OTP via email
- Receive OTP via mobile

Select the preferred authentication method and click **"Submit."**

Figure 2.2.2 – MFA Authentication Method Selection Screen



Step 3: OTP Generation and Verification

Based on the selected method:

- The system generates a One-Time Password (OTP).
- The OTP is sent to the selected channel (email or mobile).

The user is redirected to the OTP Verification Page.

Enter the received OTP and click **"Submit"**.

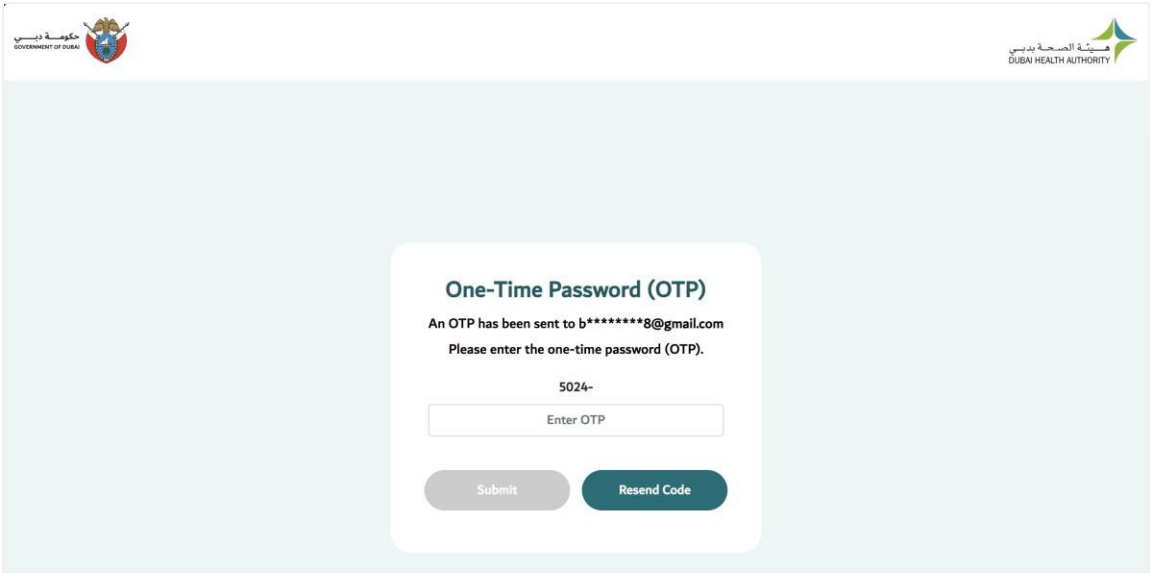


Figure 2.2.3 – OTP Verification Screen

Note:

If the OTP is valid, authentication is successful and the user proceeds to the Device Consent Page.

If the OTP is invalid or expired, an error message is displayed. The user may retry or click **"Resend Code.**

Step 4: Device Registration Consent (Optional – 15 Days)

After successful OTP verification, the system displays the Device Consent Page.

The user is given two options:

- **Register and Log In**
- **Skip and Log In**

Option 1: Register and Log In

If the user selects **"Register and Log In":**

- The current device and browser are registered.
- The MFA challenge will be remembered for 15 days on this device.
- The user is redirected to the application dashboard.

Option 2: Skip and Log In

If the user selects **"Skip and Log In"**:

- The device will not be registered.
- MFA authentication will be required during every login.
- The user is redirected to the application dashboard.

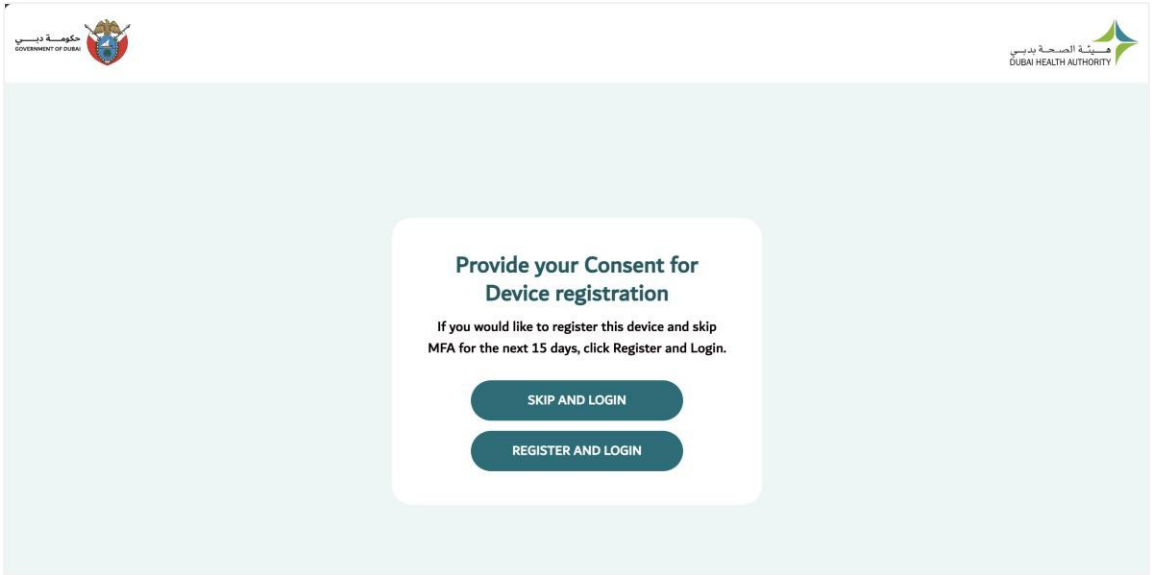


Figure 2.2.4 – Device Consent Page

2.3 Existing User Login (Unverified Email or Mobile)

This section explains the login process for existing users whose email address and/or mobile number have not yet been verified.

Users will not be allowed to access the application until all mandatory contact details are verified.

Step 1: Access the Application Login Page

Navigate to the DHA portal login page:

https://services.dha.gov.ae/

Enter your credentials: username and password.

Click **"Login"**.

Step 2: System Validation of Contact Details

After successful credential validation, the system checks the verification status of:

- Email Address
- Mobile Number

If any contact detail is unverified, the user is redirected to the respective verification page.

Verification is performed in the following order:

1. Email Address
2. Mobile Number

Scenario 1: Email and Mobile Both Unverified

The registered email address is masked and displayed on the screen.

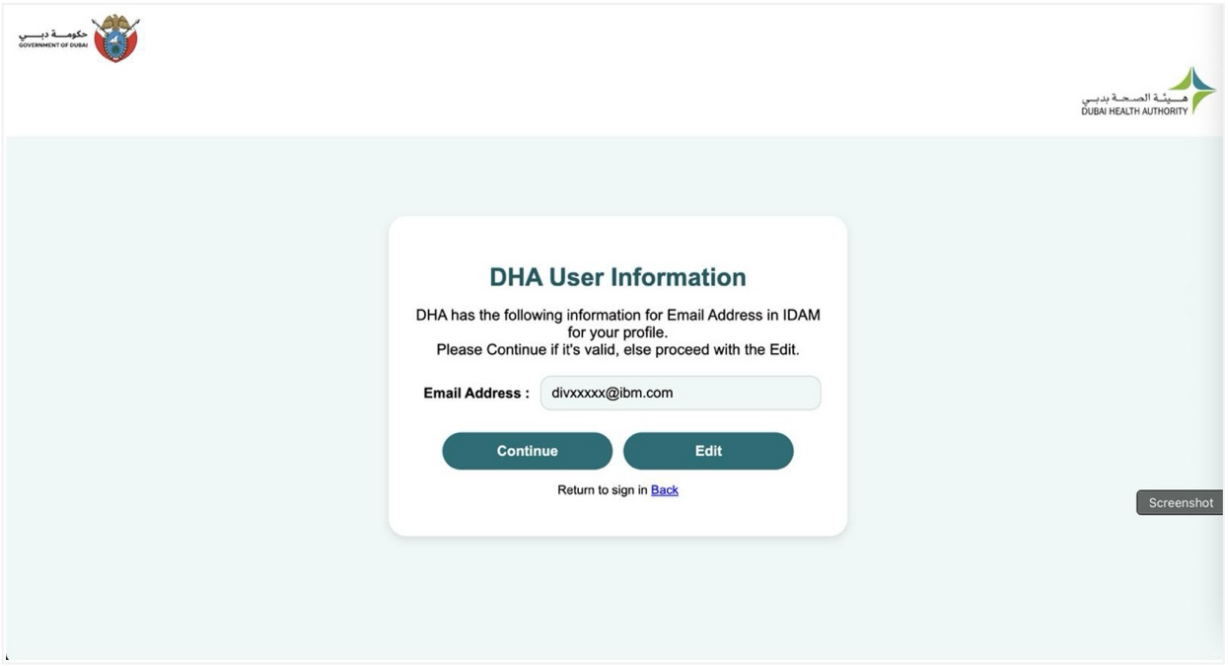
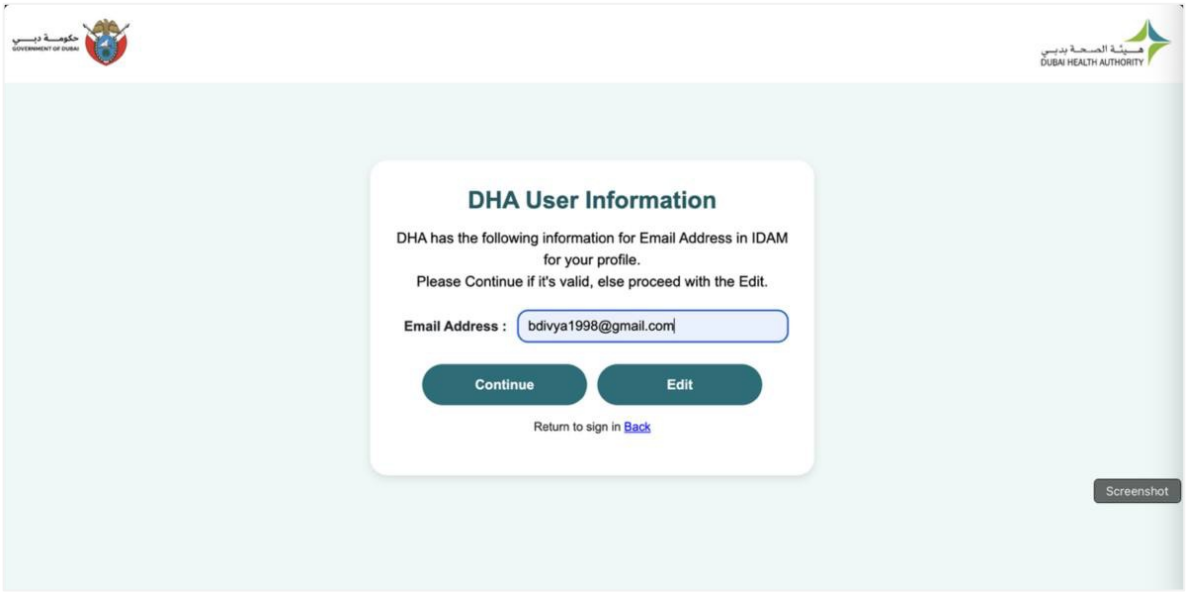


Figure 2.3.1 – Email Validation Screen

If the user needs to update the email address, click **"Edit."** The email field becomes editable.

Enter the updated email address and click **"Continue."**

A new OTP will be sent to the updated email address.



The system then redirects the user to the Email OTP Verification Page.

(Refer to Figure 2.1.2– Email OTP Verification Screen)

Enter the OTP and click **"Submit."**

After successful email verification, the user is automatically redirected to the Mobile OTP Validation Page.

- An OTP is sent to the registered mobile number.
- Enter the OTP and click **"Submit."**

After both verifications are completed, the system displays the Device Consent Page. (Refer to Figure 2.2.4– Device Consent Page.

Scenario 2: Only Mobile Unverified

If the email address is already verified:

• The system directly redirects the user to the Mobile OTP Verification Page. (Refer to Figure 2.1.3– Mobile Validation Screen).

• An OTP is sent to the registered mobile number.

• The user must enter the OTP and click “Submit.”

After successful verification of the mobile number, the system displays the Device Consent Page. The user may choose to Register and Log In or Skip and Log In.

Note:
Users cannot select which contact detail to verify first.
Access to the application is granted only after all mandatory verifications are completed.

3. Internal User Authentication Procedure

This section explains the login and multi-factor authentication process applicable to internal users accessing DHA systems.

3.1 Internal User Login

Step 1: Access the Application Login Page

Navigate to the DHA portal login page:

https://services.dha.gov.ae/

Enter the credentials: username and password

Click on **"Login".**

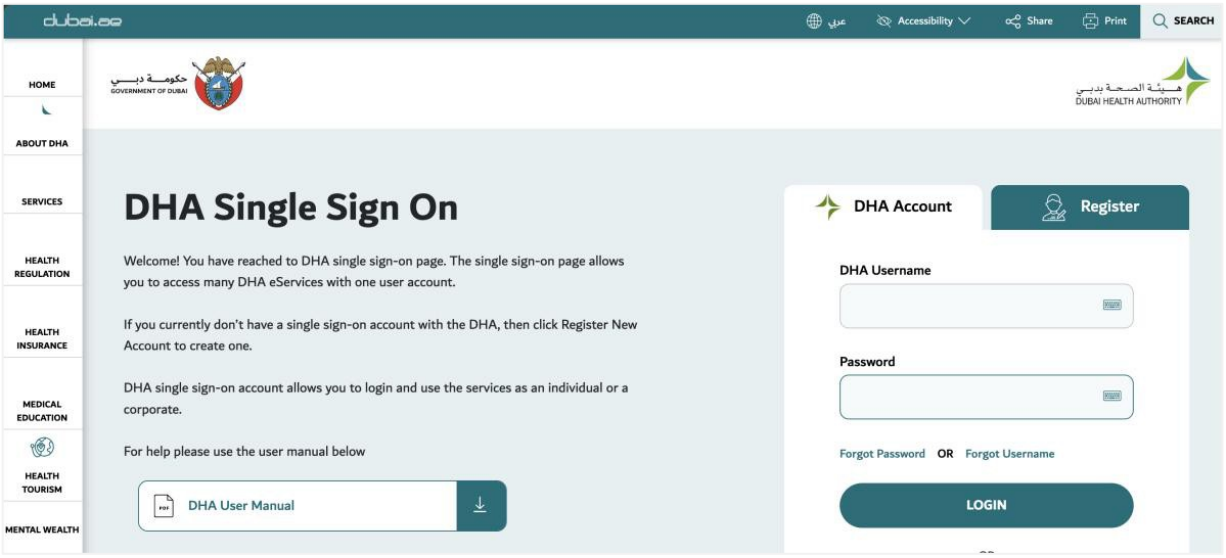


Figure 3.1.1 – Login Screen

Step 2: Multi-Factor Authentication Method Selection

After successful validation of the username and password, the system displays the **MFA Authentication Method Selection Page.**

The user must select one of the following authentication methods:

- Receive authentication code via email
- Receive authentication code via mobile
- Receive authentication code via authenticator app

Select the preferred authentication method and click **"Submit"**.

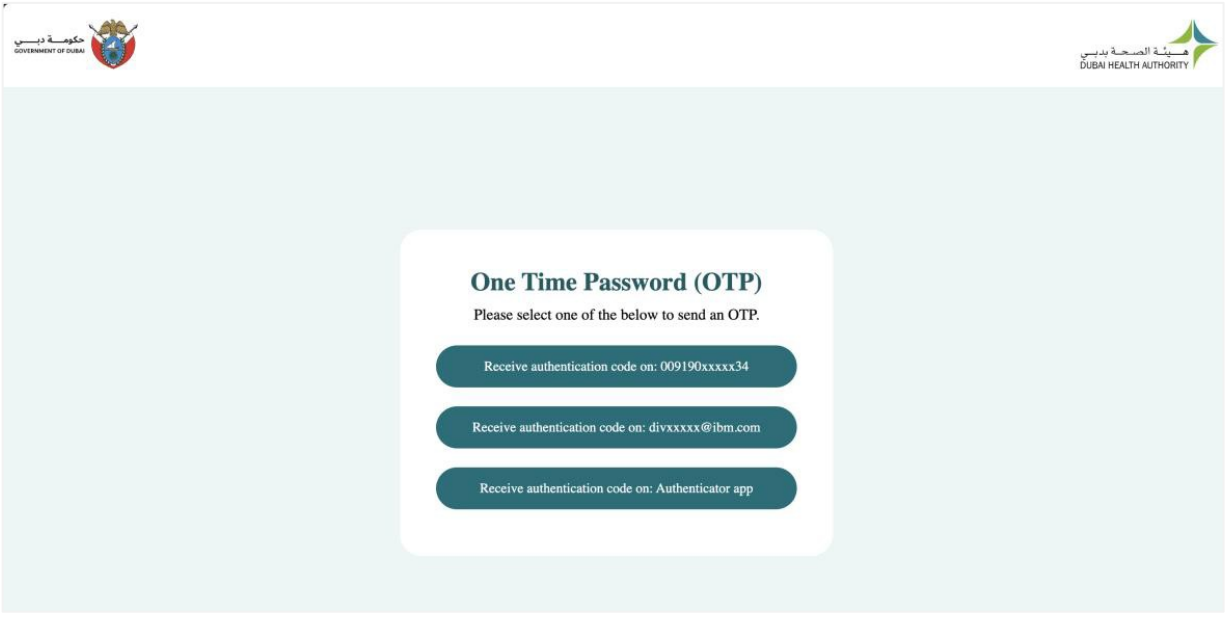


Figure 3.1.2 – Internal MFA Method Selection Screen

Step 3: OTP Authentication (Email or Mobile)

If the user selects Email OTP or Mobile OTP, the system generates a One-Time Password (OTP) and sends it to the selected channel.

The user is redirected to the OTP Verification Page.

Enter the received OTP and click **"Submit."**

(For the OTP verification screen, refer to Figure 2.2.3 – OTP Verification Screen

If the OTP is valid, authentication is successful and the system displays the Device Consent Page. (Refer to Figure 2.2.4).

Note:

Users who authenticate using email OTP or mobile OTP do not need to perform the authenticator setup steps.

Step 4: First-time enrollment (Authenticator App)

This step applies only if the user selects Receive authentication code via Authenticator App and has not previously registered an authenticator device.

The system displays a QR Code Registration Page.

- Scan the QR code using the authenticator application.
- The application generates a six-digit time-based code.
- Enter the generated code and click "Verify."

After validation, the user is redirected to the Device Consent Page. (Refer to Figure 2.2.4).

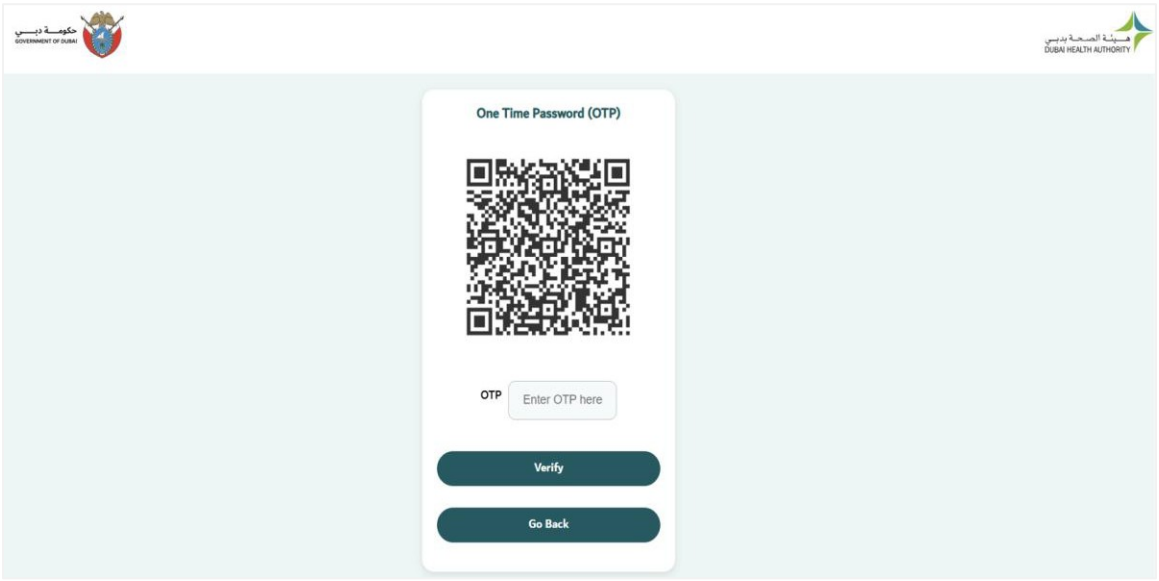


Figure 3.1.3 – TOTP QR Code Registration Screen

Note:

After successful first-time enrollment, the user will not be prompted to enter the TOTP again during the same login session.

Step 5: TOTP Authentication

This step applies to users who have already completed TOTP registration.

If the user selects **the authenticator app:**

- The system displays the TOTP Authentication Page.
- The user opens the registered authenticator application.
- The user enters the six-digit time-based code generated by the application.
- Click **"Submit."**

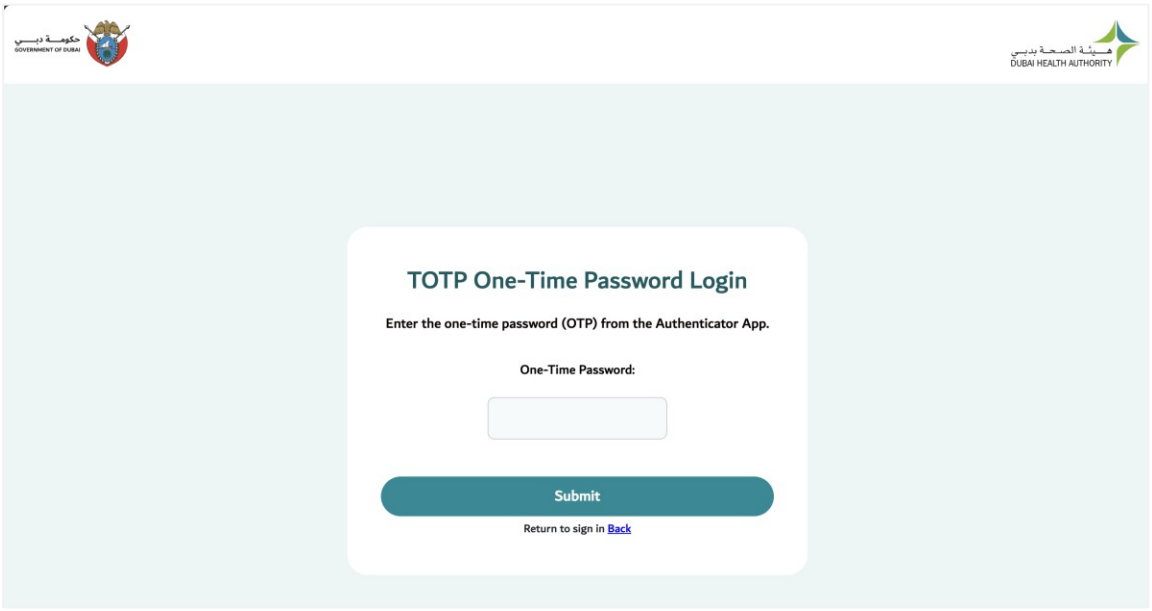


Figure 3.1.4 – TOTP Authentication Screen

Note:

If the code is valid, authentication is successful and the user proceeds to the Device Consent Page. (Refer to Figure 2.2.4).

4. OTP and Authentication Rules

This section outlines the rules and security controls applicable to OTP-based authentication.

4.1 OTP Validity

- OTPs are time-sensitive and valid only for a limited duration.
- Each OTP can be used only once.
- A newly generated OTP invalidates any previously generated OTP.

4.2 OTP Resend Limit

- Users may request a new OTP by clicking “Resend Code.”
- A maximum of five resend attempts is allowed.
- On the sixth attempt, the system displays an error message indicating:

  “You have reached the maximum number of resend attempts. Please try again later.”
- The user must wait for the defined cooldown period before requesting another OTP.

4.3 Invalid OTP Attempts

If an incorrect OTP is entered:

- The system displays an error message such as: “The submitted One-Time Password is invalid.”
- The system also displays the number of remaining attempts.
- If the maximum number of invalid attempts is exceeded, the account may be temporarily restricted.

4.4 TOTP (Authenticator App) Rules

- TOTP codes refresh automatically at fixed intervals (typically every 30 seconds).
- If the entered TOTP expires, the user must enter the newly generated code.
- TOTP codes cannot be resent.
- Ensure that the device time is synchronised automatically for accurate validation.

Tel 800342 | P.O. Box 4545 Dubai, UAE | dha.gov.ae | info@dha.gov.ae | ص.ب. 4545 دبي إ ع م | هاتف 800 342

4.5 Device Registration Validity

- If the user selects **"Register and Log In",** the device is trusted for **15 days.**
- During this period, the user will not be prompted for MFA when logging in from the same device and browser.
- After 15 days, MFA authentication will be required again.

4.6 Submit Button Behaviour

- The "Submit" button remains disabled until a valid OTP format is entered in the input field.
- The user must enter the required OTP digits before submission is allowed.

Tel 800342 | P.O. Box 4545 Dubai, UAE | dha.gov.ae | info@dha.gov.ae | ص.ب. 4545 دبي إ ع م | هاتف 800 342

5. Frequently Asked Questions (FAQs)

Q1. What should I do if I do not receive the OTP?

- Check your email spam or junk folder.
- Verify that your registered mobile number or email address is correct.
- Click **"Resend Code."**
- Ensure that the resend limit has not been exceeded.

Q2. How many times can I request a new OTP?

A maximum of five resend attempts is allowed.

After exceeding the limit, you must wait for the cooldown period before requesting another OTP.

Q3. What happens if I enter the wrong OTP multiple times?

The system displays the number of remaining attempts.

If the maximum number of invalid attempts is exceeded, the account may be temporarily restricted.

Q4. Why am I asked to scan a QR code?

The QR code is required for first-time registration of the Authenticator App (TOTP).

After successful registration, future logins require only the six-digit code generated by the application.

Q5. I selected "Register and Log In," but I am still asked for MFA on another device. Why?

Device registration applies only to the specific device and browser used during registration.

If you log in from a different device or browser, MFA authentication will be required.

Q6. What happens if I clear my browser cache or cookies?

Clearing browser data removes the trusted device information.

You will be required to complete MFA authentication again.

Tel 800342 | P.O. Box 4545 Dubai, UAE | dha.gov.ae | info@dha.gov.ae | ص.ب. 4545 دبي إ ع م | هاتف 800 342

Q7. Can I change my email or mobile number during verification?

Yes, but only for external users.

You can update your email address using the **"Edit"** option on the Email Validation Page or update your mobile number on the Mobile Validation Page before requesting the OTP.

Q8. What should I do if my Authenticator App is not generating valid codes?

- Ensure your device time is set automatically.
- Try entering the newly refreshed code.
- If the issue persists, contact IT support.

Q9. Can I change my email or mobile number after verification?

No. You must contact the DHA Help Desk to request this change.

Tel 800342 | P.O. Box 4545 Dubai, UAE | dha.gov.ae | info@dha.gov.ae | ص.ب. 4545 دبي إ ع م | هاتف 800 342