

SUPPLIER LOGIN AND AUTHENTICATION WORK INSTRUCTIONS

Abbreviations

QF – Qatar Foundation

ERP – QF's internal Enterprise Resource Planning system

PD – QF Procurement Directorate

MFA – Multi Factor Authentication

OTP – One-Time Password

TOTP – Time-based OTP

IDCS – Oracle Identity Cloud Services

IDAM – Oracle Identity & Access Management

Contents

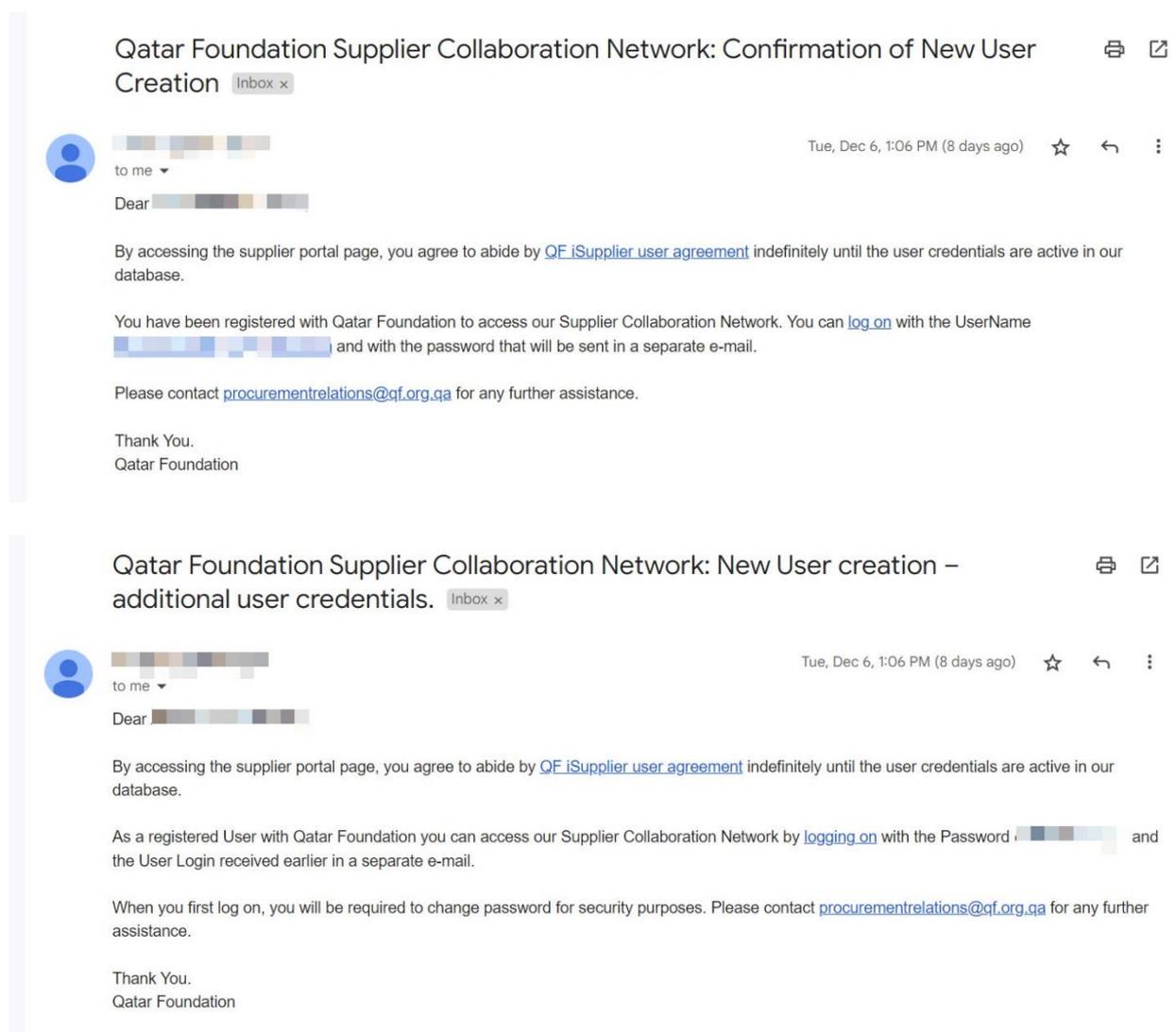
| | |
|--|----|
| Abbreviations | 2 |
| Fusion Login Instructions | 4 |
| FIRST TIME LOGIN TO ERP | 4 |
| SECOND TIME LOGIN | 9 |
| IDCS LOGIN (MULTIPLE APPLICATION ACCESS) | 11 |
| Multi Factor Authentication (MFA) | 12 |
| ADD MFA OPTIONS | 12 |
| RESET PASSWORD | 14 |
| RESET MFA | 16 |

Fusion Login Instructions

First Time Login to ERP

When a user is registered as a contact for the supplier with access to iSupplier portal, you will receive separate emails with your username and password. Please note that the password needs to be changed during the first login.

Registration Email



The image shows two screenshots of registration emails. The first email is titled "Qatar Foundation Supplier Collaboration Network: Confirmation of New User Creation" and the second is titled "Qatar Foundation Supplier Collaboration Network: New User creation – additional user credentials." Both emails are dated "Tue, Dec 6, 1:06 PM (8 days ago)".

Qatar Foundation Supplier Collaboration Network: Confirmation of New User Creation

to me

Dear [redacted]

By accessing the supplier portal page, you agree to abide by [QF iSupplier user agreement](#) indefinitely until the user credentials are active in our database.

You have been registered with Qatar Foundation to access our Supplier Collaboration Network. You can [log on](#) with the UserName [redacted] and with the password that will be sent in a separate e-mail.

Please contact procurementrelations@qf.org.qa for any further assistance.

Thank You.
Qatar Foundation

Qatar Foundation Supplier Collaboration Network: New User creation – additional user credentials.

to me

Dear [redacted]

By accessing the supplier portal page, you agree to abide by [QF iSupplier user agreement](#) indefinitely until the user credentials are active in our database.

As a registered User with Qatar Foundation you can access our Supplier Collaboration Network by [logging on](#) with the Password [redacted] and the User Login received earlier in a separate e-mail.

When you first log on, you will be required to change password for security purposes. Please contact procurementrelations@qf.org.qa for any further assistance.

Thank You.
Qatar Foundation

Go to the ERP Application Login page - <https://suppliers.qf.org.qa/>

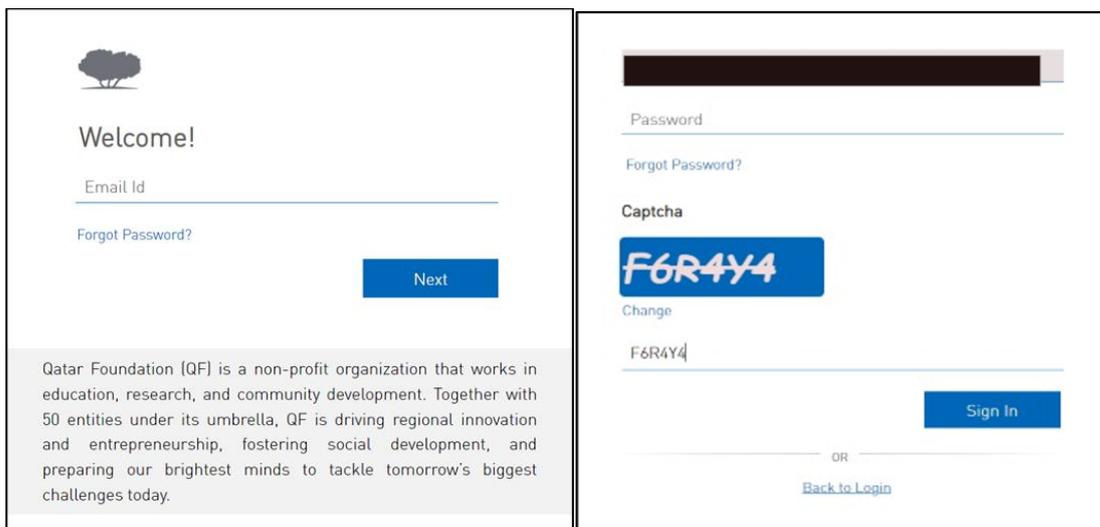
Login / Authentication

Step 1: Enter username that is received in Registration Email.

Step 2: Enter initial login Password.

Step 3: Enter Captcha

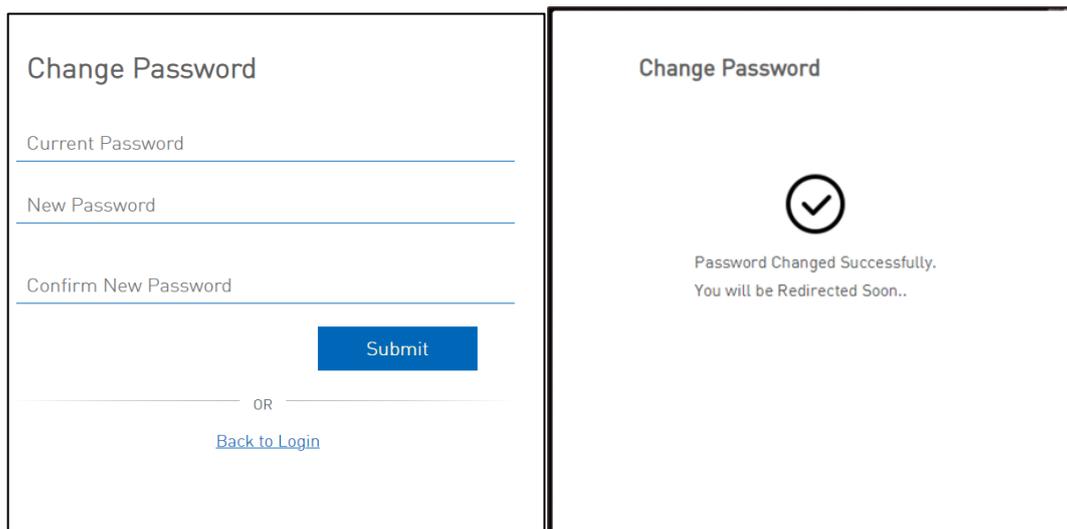
Step 4: Click Sign In button.



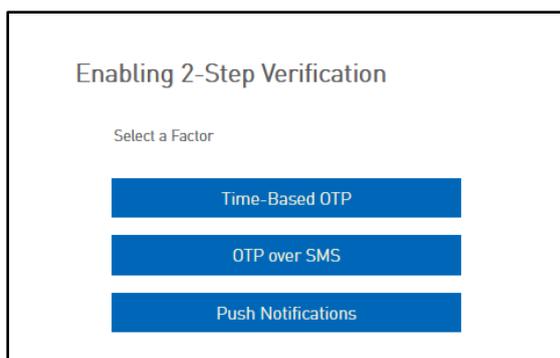
Change Password

Step 1: Enter old password & new password twice.

Step 2: Click on Submit

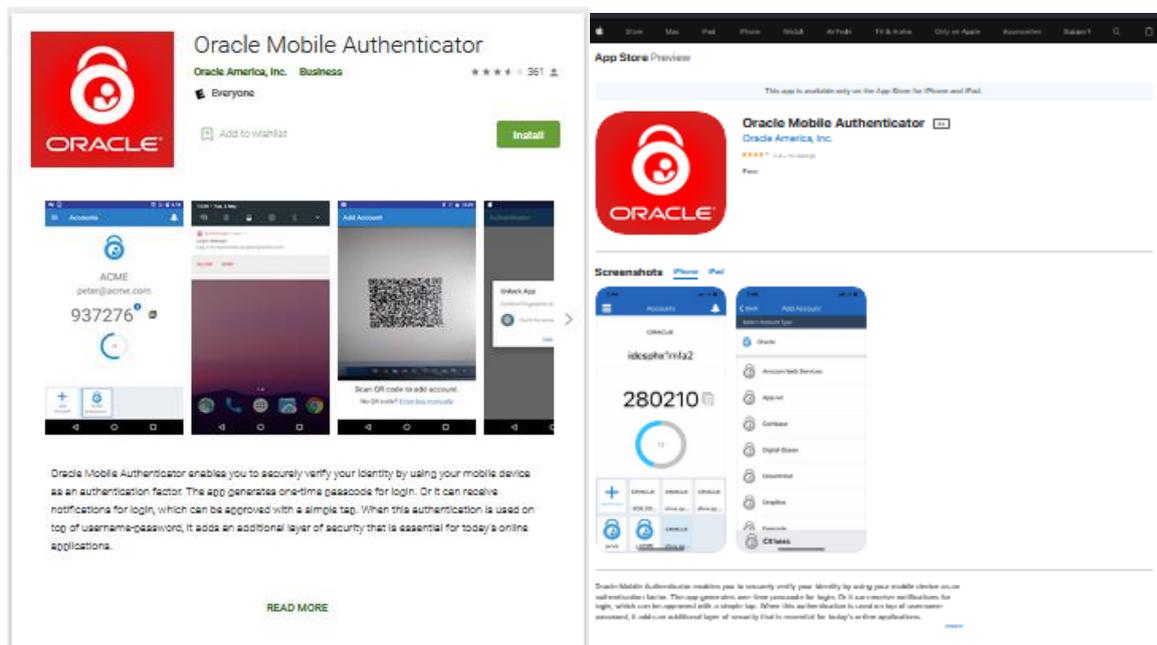


Setup MFA



Chose Any One of the above-mentioned methods.

Note: Download the Oracle Mobile Authenticator App from the App store for Time-Based OTP and Push Notification method

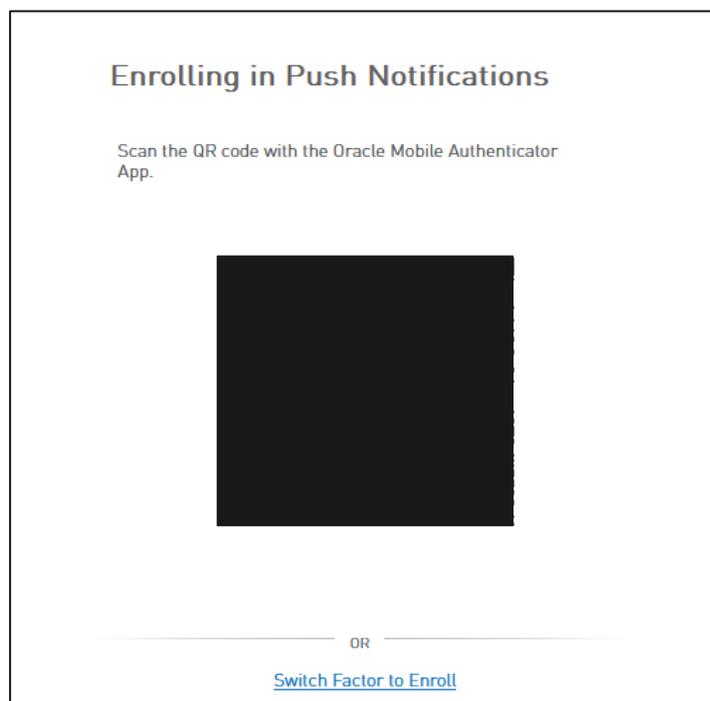


Push Notification Method

Step 1: Open the Oracle Mobile Authenticator App on Mobile.

Step 2: Click on Add Button in Oracle Authenticator App.

Step 3: Scan the QR Code which is visible on your login screen.



Time based OTP (TOTP) Method

Step 1: Open the Oracle mobile Authenticator app on mobile.

Step 2: Click on Add Button In authenticator app.

Step 3: Scan QR code which is visible on your login screen.

Step 4: Type the Time-based OTP

Step 5: Click on Enroll Button

Enrolling in Time-based OTP

Scan the QR code with the Oracle Mobile Authenticator App.
Then enter the code you see on your phone's screen in the field below.



Time-based OTP Code

[Enroll](#)

Note: Kindly contact IT Service Desk at +974 4454 0070 or send an email to itsupport@qf.org.qa in case of any difficulties.

OR

[Switch Factor to Enroll](#)

OTP over SMS Method

Step 1: Select Country

Step 2: Enter Mobile Number and click on Enroll.

Step 3: Enter OTP Received on Mobile Number

Step 4: Click On Verify

Enrolling in OTP over SMS

Please enter mobile number to send SMS

Country Code:

Mobile Number

[Enroll](#)

Note: Kindly contact IT Service Desk at +974 4454 0070 or send an email to itsupport@qf.org.qa if any Country Code is Incorrect.

OR

[Switch Factor to Enroll](#)

Verifying OTP

Please enter OTP code sent to
+91XXXXXXXX470

OTP

[Verify](#)

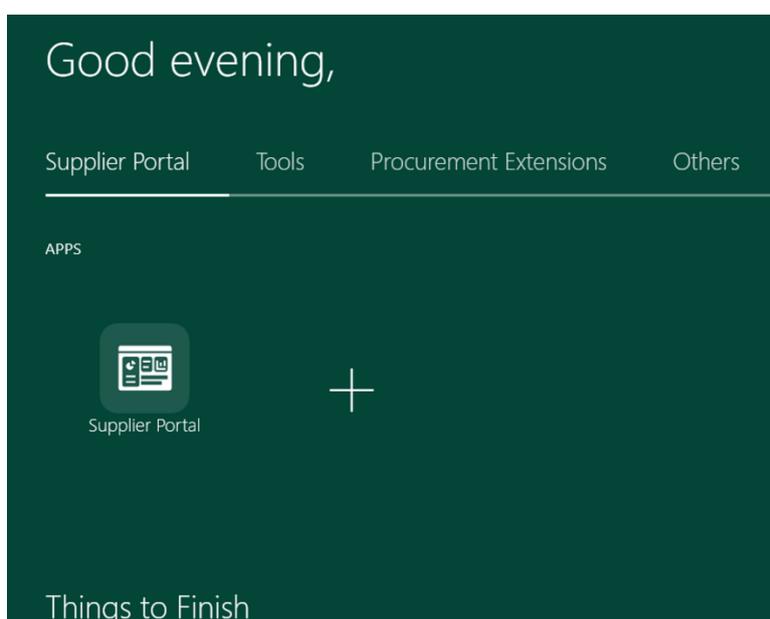
Did not get the SMS?
[Resend SMS](#)

Note: Kindly contact IT Service Desk at +974 4454 0070 or send an email to itsupport@qf.org.qa in case of any difficulties.

OR

[Switch Factor to Enroll](#)

User redirected to Fusion console.



Second Time Login

Go to the ERP Application Login page - <https://suppliers.qf.org.qa/>

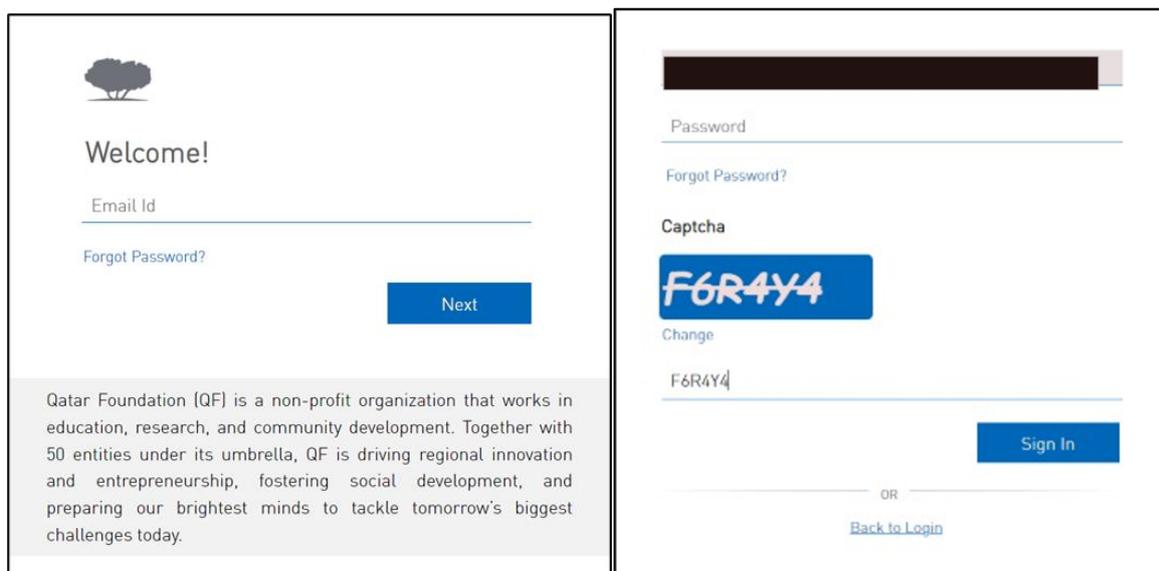
Login / Authentication

Step 1: Enter username received in Registration Email.

Step 2: Enter the New Password (set during the first-time login)

Step 3: Enter Captcha

Step 4: Click Sign In button.



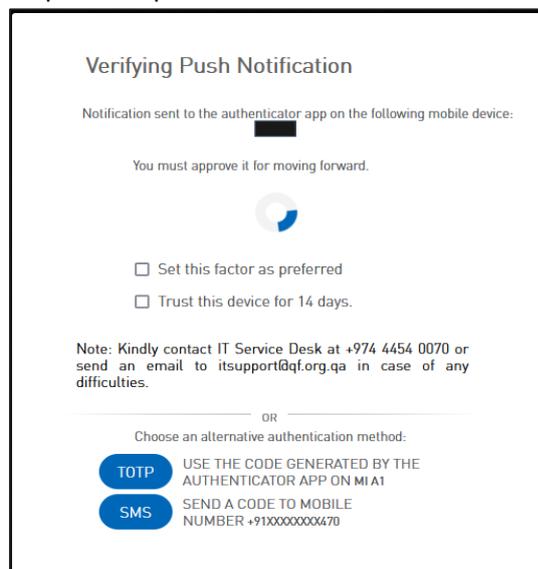
The image shows two side-by-side screenshots of the login interface. The left screenshot is the 'Welcome!' page, featuring a tree logo, the text 'Welcome!', and input fields for 'Email Id' and 'Forgot Password?'. A blue 'Next' button is positioned below the 'Email Id' field. At the bottom, there is a paragraph of text about the Qatar Foundation (QF). The right screenshot is the authentication page, showing a redacted 'Password' field, a 'Forgot Password?' link, a 'Captcha' field with a blue box containing the text 'F6R4Y4', and a 'Sign In' button. Below the 'Sign In' button, there is an 'OR' separator and a 'Back to Login' link.

Verify MFA

Verify Your Identity using enrolled method.

- Using Push Notification

Step 1: Accept Push Notification on Mobile Authenticator



The image shows a screenshot of the 'Verifying Push Notification' screen. At the top, it says 'Verifying Push Notification'. Below that, it states 'Notification sent to the authenticator app on the following mobile device:' followed by a redacted device name. A message says 'You must approve it for moving forward.' with a circular progress indicator. There are two checkboxes: 'Set this factor as preferred' and 'Trust this device for 14 days.'. At the bottom, there is a note: 'Note: Kindly contact IT Service Desk at +974 4454 0070 or send an email to itsupport@qf.org.qa in case of any difficulties.' Below the note, there is an 'OR' separator and the text 'Choose an alternative authentication method:'. There are two buttons: 'TOTP' with the text 'USE THE CODE GENERATED BY THE AUTHENTICATOR APP ON MIA1' and 'SMS' with the text 'SEND A CODE TO MOBILE NUMBER +91XXXXXXXXX670'.

- **Using TOTP**

Step 1: Enter OTP Displayed on Mobile Authenticator

Step 2: Click On Verify

Verifying Time-based OTP

Please enter Time-based OTP as displayed in 

 Trust this device for 14 days.

Note: Kindly contact IT Service Desk at +974 4454 0070 or send an email to itsupport@qf.org.qa in case of any difficulties.

OR

[Use an alternative authentication method](#)

- **Using OTP over SMS**

Step 1: Enter OTP Received on Mobile Number

Step 2: Click On Verify

Verifying Push Notification

Notification sent to the authenticator app on the following mobile device:
MI A1

You must approve it for moving forward.


 Set this factor as preferred
 Trust this device for 14 days.

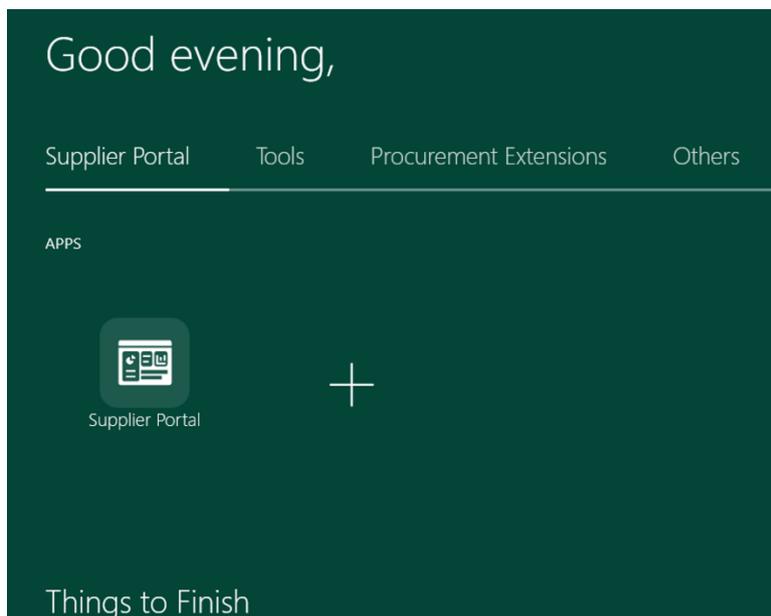
Note: Kindly contact IT Service Desk at +974 4454 0070 or send an email to itsupport@qf.org.qa in case of any difficulties.

OR

Choose an alternative authentication method:

| | |
|-------------------------------------|--|
| <input type="button" value="TOTP"/> | USE THE CODE GENERATED BY THE AUTHENTICATOR APP ON MI A1 |
| <input type="button" value="SMS"/> | SEND A CODE TO MOBILE NUMBER +91XXXXXXXXX470 |

User redirected to Fusion console.



IDCS Login (Multiple Application Access)

- User visits the URL: <https://login.qf.org.qa/>.

IDCS Login / Authentication

Step 1: Enter username received in Registration Email.

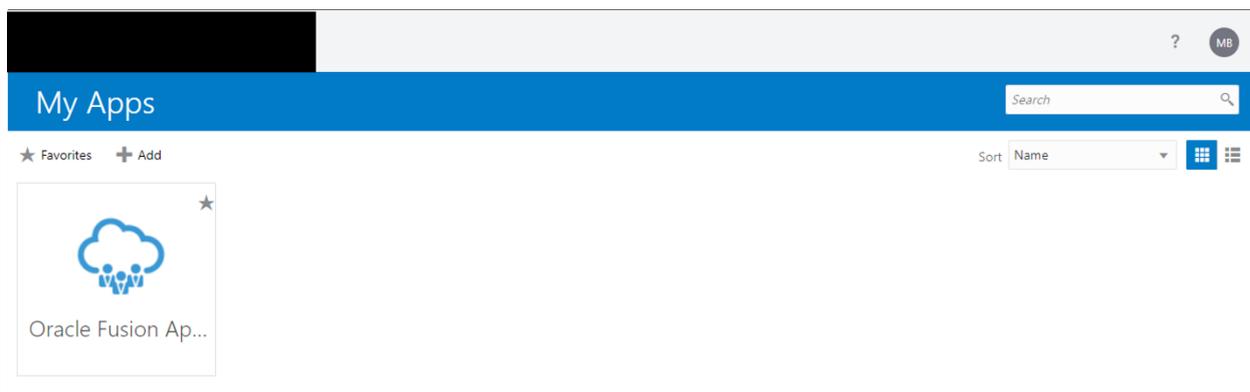
Step 2: Enter your Password.

Step 3: Enter Captcha

Step 4: Click Sign In button.

| | |
|--|---|
|  <p>Welcome!</p> <p>Email Id <input type="text"/></p> <p>Forgot Password?</p> <p>Next</p> <p>Qatar Foundation (QF) is a non-profit organization that works in education, research, and community development. Together with 50 entities under its umbrella, QF is driving regional innovation and entrepreneurship, fostering social development, and preparing our brightest minds to tackle tomorrow's biggest challenges today.</p> | <input type="password"/> <p>Password</p> <p>Forgot Password?</p> <p>Captcha</p> <p>F6R4Y4</p> <p>Change</p> <p><input type="text" value="F6R4Y4"/></p> <p>Sign In</p> <p>OR</p> <p>Back to Login</p> |
|--|---|

IDCS My Apps Page



Users can view the application tiles that they have access to. Click on the relevant tile to access that application.

Multi Factor Authentication (MFA)

Add MFA Options

Login to IDCS (click on the below URL)

- URL: <https://login.qf.org.qa/>

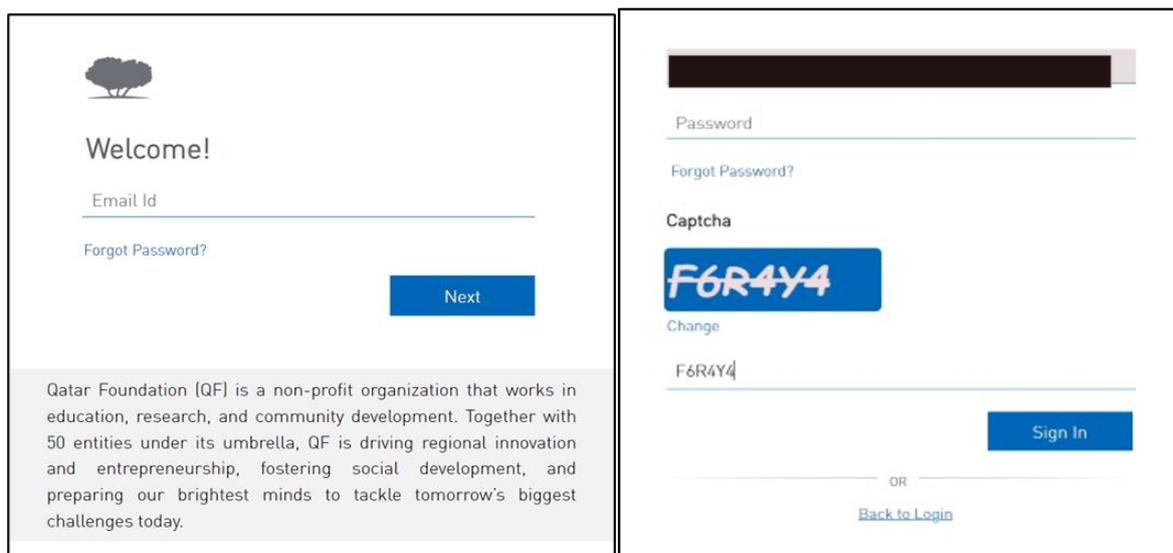
IDCS Login / Authentication

Step 1: Enter username that is received in Registration Email.

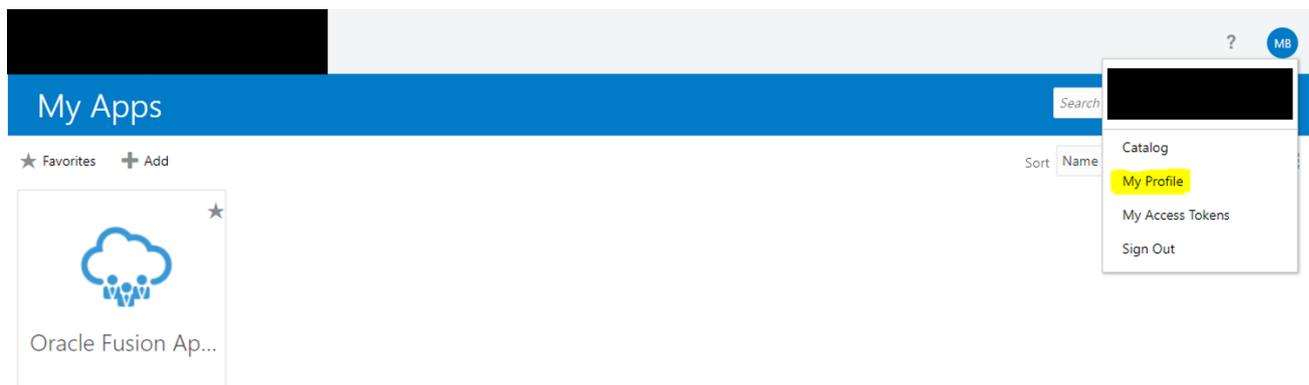
Step 2: Enter your Password.

Step 3: Enter Captcha

Step 4: Click Sign In button.

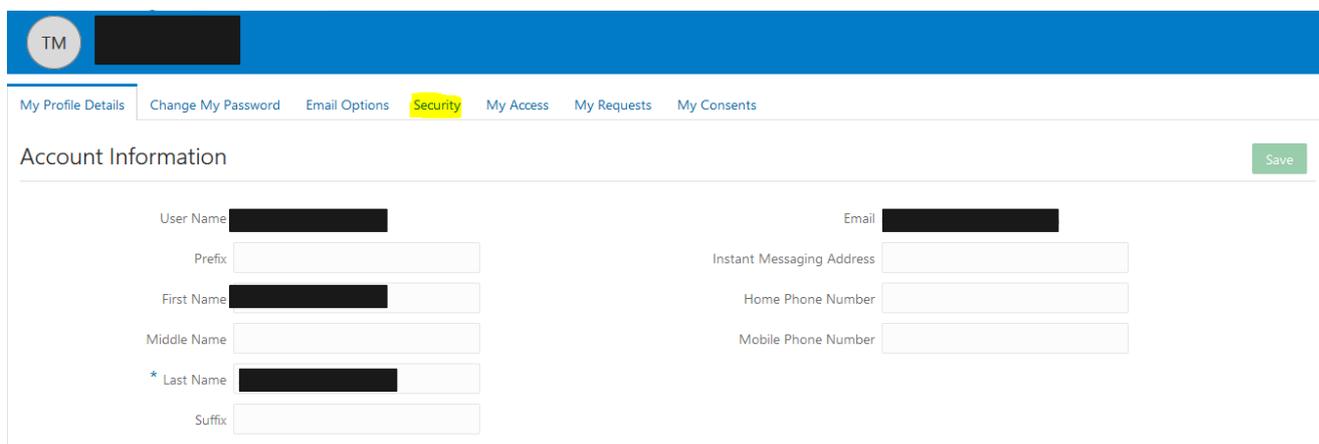


Go to My Profile



The screenshot shows the 'My Apps' section of the user interface. A dropdown menu is open, showing options: 'Catalog', 'My Profile' (highlighted), 'My Access Tokens', and 'Sign Out'. Below the menu, there is a search bar and a 'Sort' button. A card for 'Oracle Fusion Ap...' is visible, featuring a cloud icon and a star.

Go to Security Section



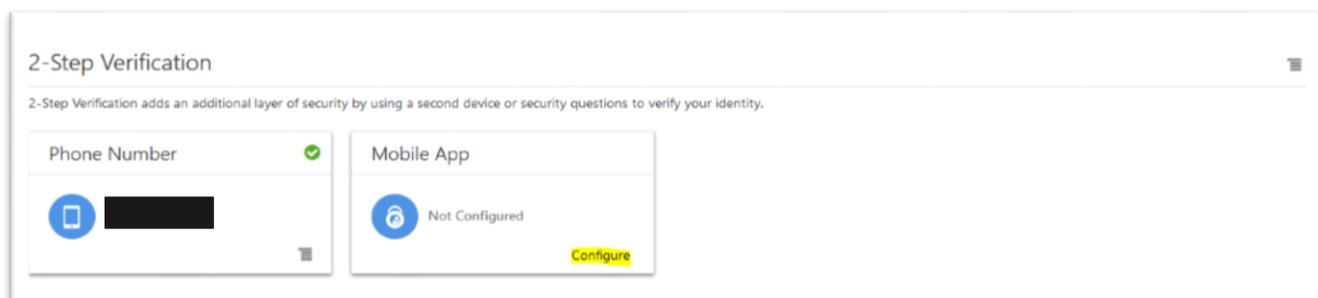
The screenshot shows the 'Security' section of the user interface. The 'Security' tab is selected in the navigation bar. Below the navigation bar, there is a 'Save' button. The 'Account Information' section contains several input fields for user details:

- User Name: [Redacted]
- Prefix: [Input Field]
- First Name: [Redacted]
- Middle Name: [Input Field]
- * Last Name: [Redacted]
- Suffix: [Input Field]
- Email: [Redacted]
- Instant Messaging Address: [Input Field]
- Home Phone Number: [Input Field]
- Mobile Phone Number: [Input Field]

Configure MFA

Configure option will be visible for the MFA Factors, which have not been configured yet.

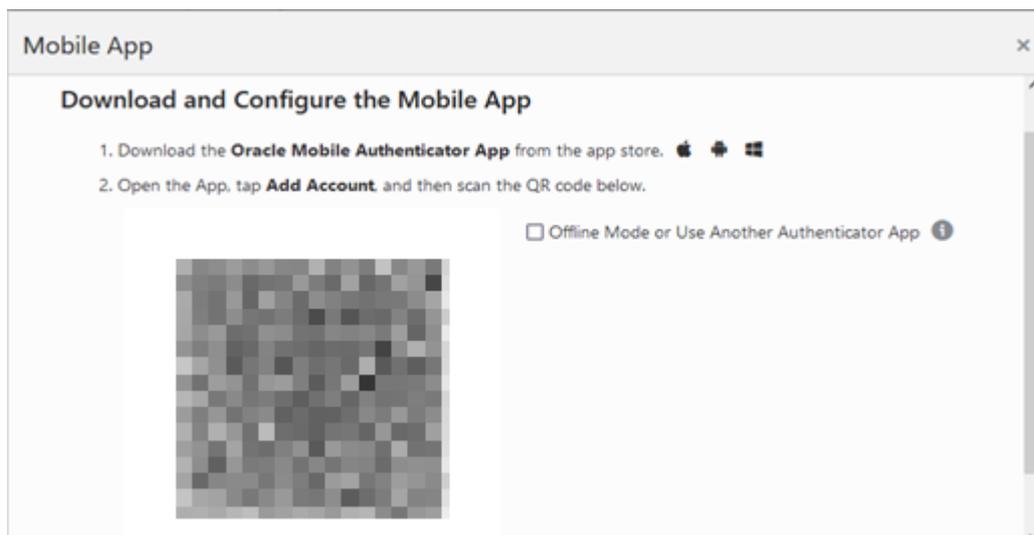
Note: As shown in the screenshot the SMS OTP option was already configured so there is configure button only for Mobile App,



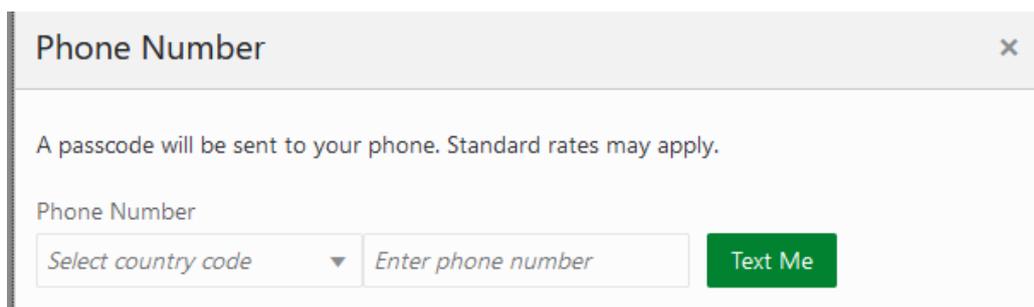
The screenshot shows the '2-Step Verification' section of the user interface. It displays two options for MFA factors:

- Phone Number: [Configured] (indicated by a green checkmark)
- Mobile App: [Not Configured] (indicated by a blue padlock icon and a 'Configure' button)

Scan the QR Code using Oracle Mobile Authenticator



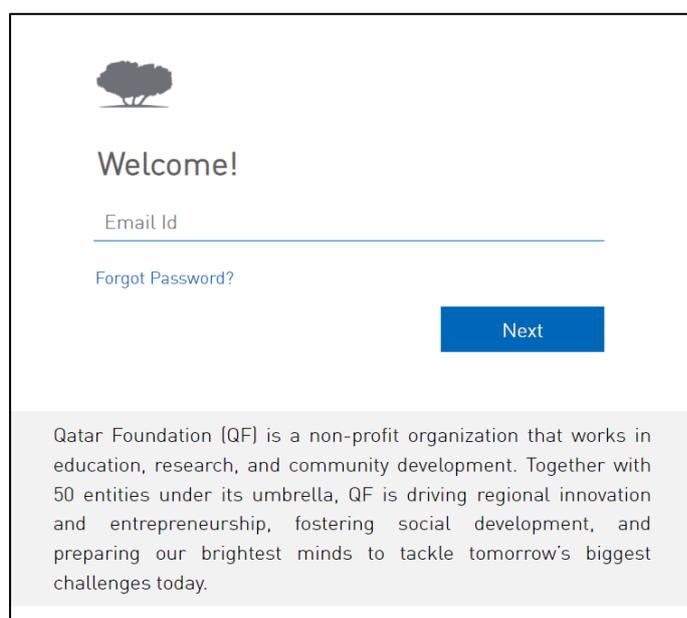
Configure Mobile Number for SMS OTP



Reset Password

Step 1: Visit this Fusion login URL: <https://suppliers.qf.org.qa/>

Step 2: Click on forgot password.



Step 3: Enter your Email id.

Step 4: Click on Next. Password reset mail is sent to the mail id provided.

| | |
|---|--|
| <p>Forgot your Password?</p> <p>Please, enter Email Id for password reset.</p> <p>Email Id <input type="text"/></p> <p><input type="submit" value="Submit"/></p> <p>OR</p> <p>Back to Login</p> | <p>Forgot your Password?</p> <p>Password reset email has been sent for username: [REDACTED]</p> <p>If you don't receive an email, this could mean you signed up with a different email address.</p> <p>Incorrect UserName? Fix UserName</p> <p>Did not get the email? Resend email</p> |
|---|--|

Step 5: Click on Password Reset Link in email.



Dear [REDACTED]

On [REDACTED] you requested to reset your password. You must reset your password by clicking on below password reset button.

[Password Reset](#)

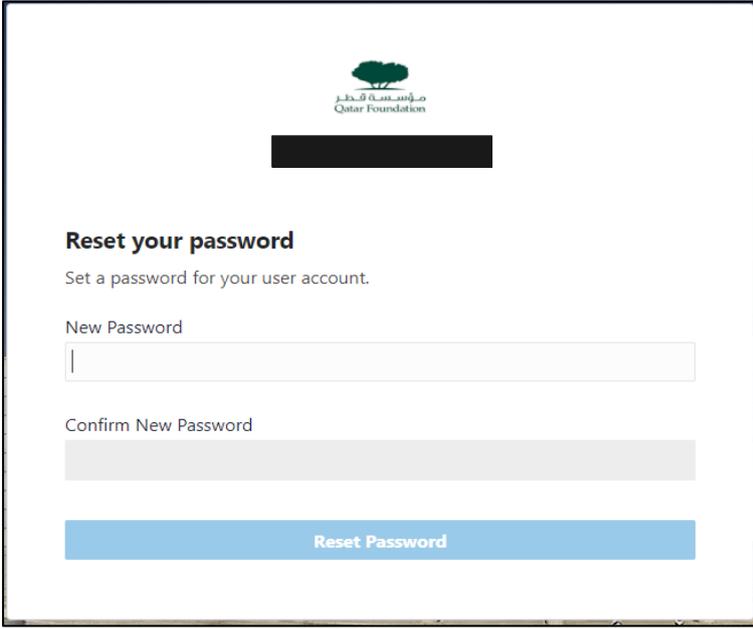
Details

If the [Password Reset](#) link doesn't work, please copy and paste the following URL into the address bar of your browser:

[REDACTED]

Important: This link will expire on Friday, December 16, 2022 8:20:55 AM AST. Also, if you don't recognize this message, please contact IT Service Desk at +974 4454 0070 or send an email to itsupport@qf.org.qa.

Regards,
QF Identity Administrator



The screenshot shows a web form for resetting a password. At the top, there is the Qatar Foundation logo and a blacked-out area. Below that, the heading "Reset your password" is followed by the instruction "Set a password for your user account." There are two input fields: "New Password" and "Confirm New Password". A blue button labeled "Reset Password" is at the bottom of the form.

Step 6: Enter New Password

Step 7: Confirm New Password

Step 8: Click on Reset Password

Reset MFA

Step 1: Send an email to QF ITSC (itsupport@qf.org.qa) requesting to reset MFA.

Step 2: ITSC will raise a ticket and will be assigned to IDAM Team

Step 3: MFA factor would be Reset.

Step 4: In the next login the user can setup the MFA with the new mobile number or with a different device using Oracle Mobile Authenticator Application. Check the "[Add MFA Options](#)" section above for the detailed steps.