

MIMS: MOE IDENTITY MANAGEMENT SYSTEM



Multi-Factor Authentication

A PRESENTATION BY
MINISTRY OF EDUCATION, SINGAPORE

TABLE OF CONTENTS

1. Login to MIMS Authenticator Module
2. Soft Token (OTP)
3. FAQ

1. MIMS Authenticator Module

Login to MIMS Authenticator Module

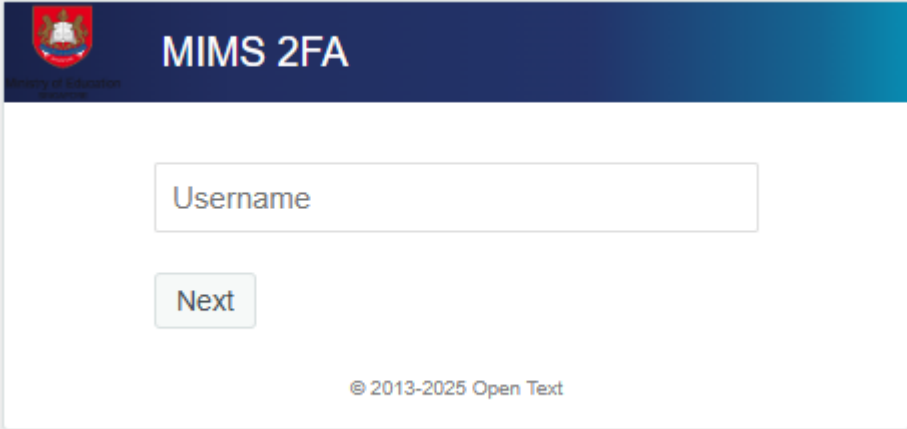
Step 1: Access to authentication module

a. Go to URL: <https://auth.mims.moe.gov.sg/account/auth>

b. Input MIMS Login ID and click “Next” button.

School user : username@schools.gov.sg

HQ user : username@hq.moe.gov.sg



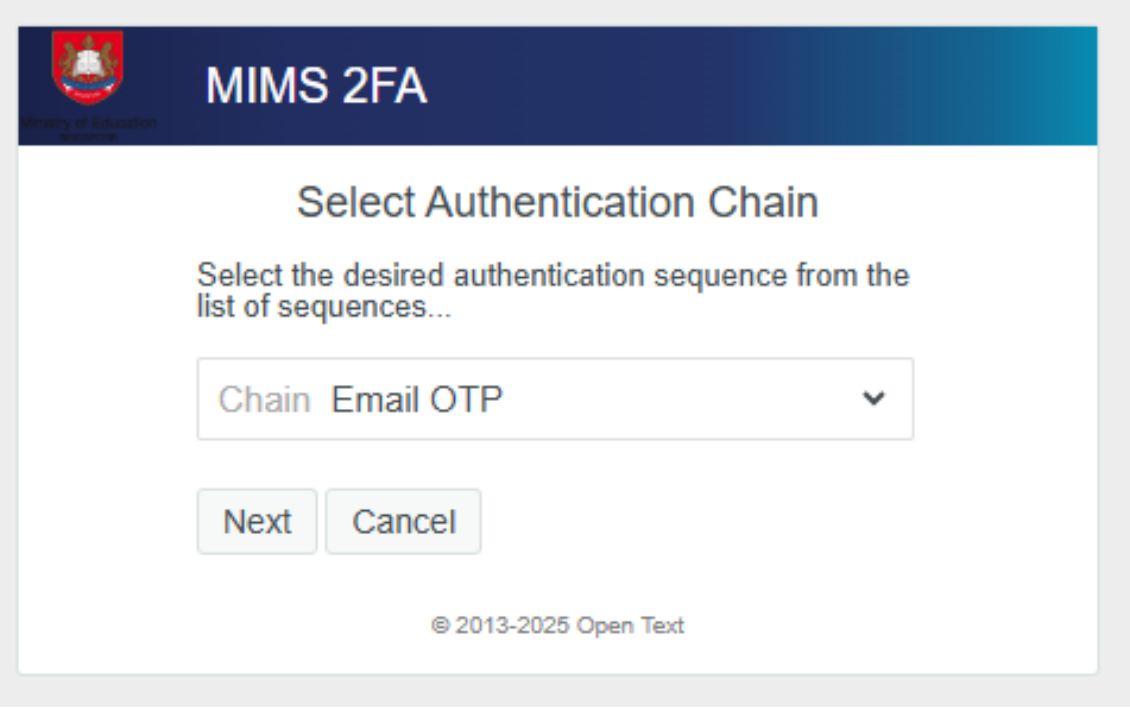
The screenshot shows the MIMS 2FA login interface. At the top, there is a dark blue header with the Ministry of Education Singapore logo on the left and the text "MIMS 2FA" on the right. Below the header, there is a white rectangular box containing a text input field labeled "Username" and a "Next" button below it. At the bottom of the white box, there is a copyright notice: "© 2013-2025 Open Text".

Login to MIMS Authenticator Module

Step 2: Login with Email OTP (Default)

a. Under Chain, select “Email OTP” option and click “Next” button

Note : an email OTP will be sent to your MIMS Primary Email address



The screenshot shows the MIMS 2FA login interface. At the top, there is a dark blue header with the MIMS logo on the left and the text 'MIMS 2FA' on the right. Below the header, the main content area is white. It features the title 'Select Authentication Chain' in a bold, dark blue font. Underneath the title, there is a smaller line of text: 'Select the desired authentication sequence from the list of sequences...'. Below this text is a dropdown menu with the text 'Chain Email OTP' and a downward-pointing arrow. At the bottom of the form, there are two buttons: 'Next' and 'Cancel'. At the very bottom of the page, there is a small copyright notice: '© 2013-2025 Open Text'.

Login to MIMS Authenticator Module

Step 3: Input the OTP received in your email
The Email OTP will expired after 15 mins.

Login OTP



MOE_DXD_MIMS@moe.gov.sg



To: [Redacted]

External Message: Please be cautious when opening links or attachments in email

Use **OTP 386328**, #7 to login as [Redacted]@hq.moe.gov.sg from OSP to Authenticators Management

Thank you!

Received, thank you.

Got it, thanks!



Reply



Forward

 **MIMS IZ 2FA**

One-Time Authentication Code (OTP)

OTP #7 sent to m*****_ag@nec.com.sg

Show

Next

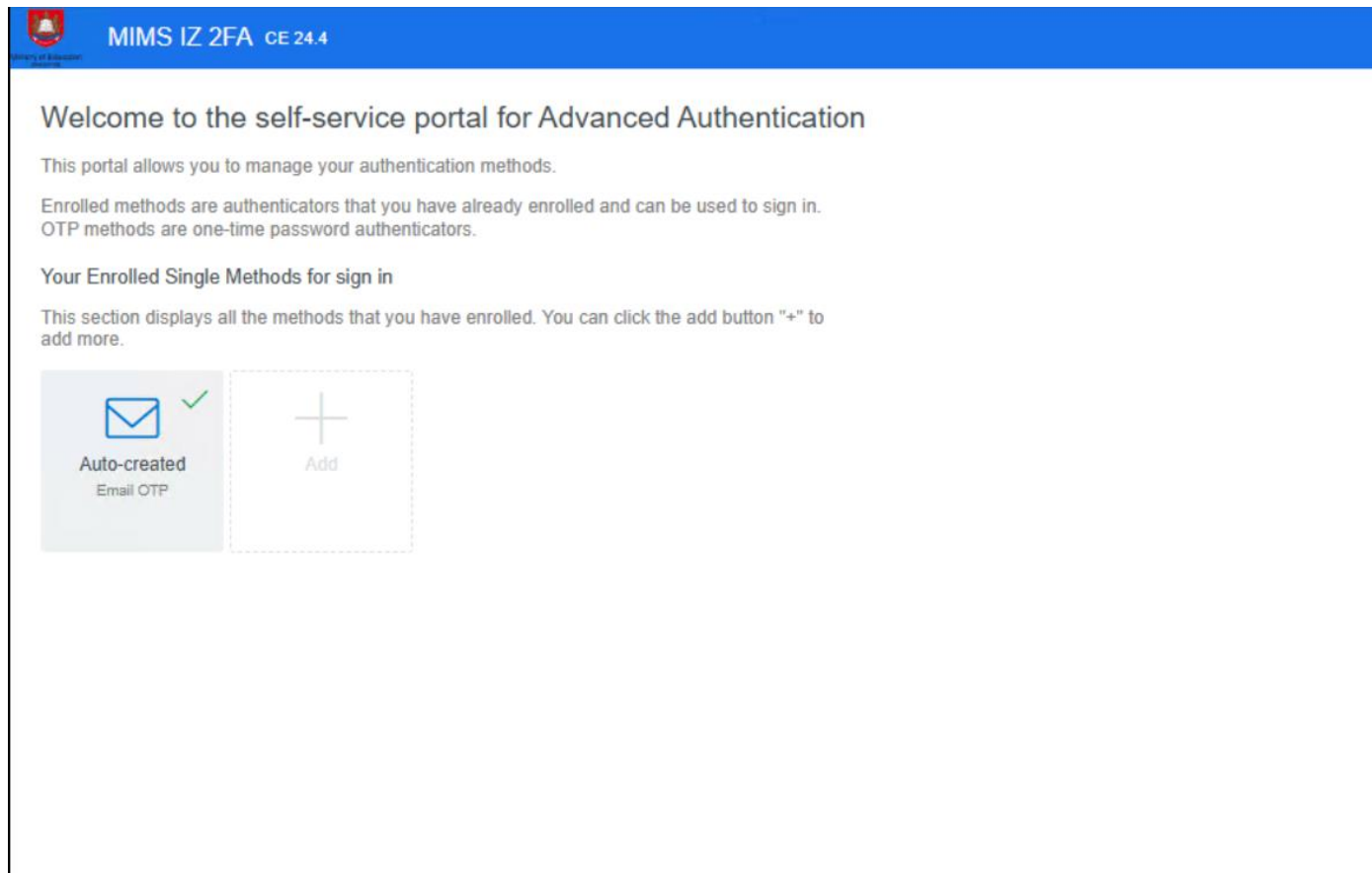
Resend

Cancel

© 2013-2025 Open Text

Login to MIMS Authenticator Module

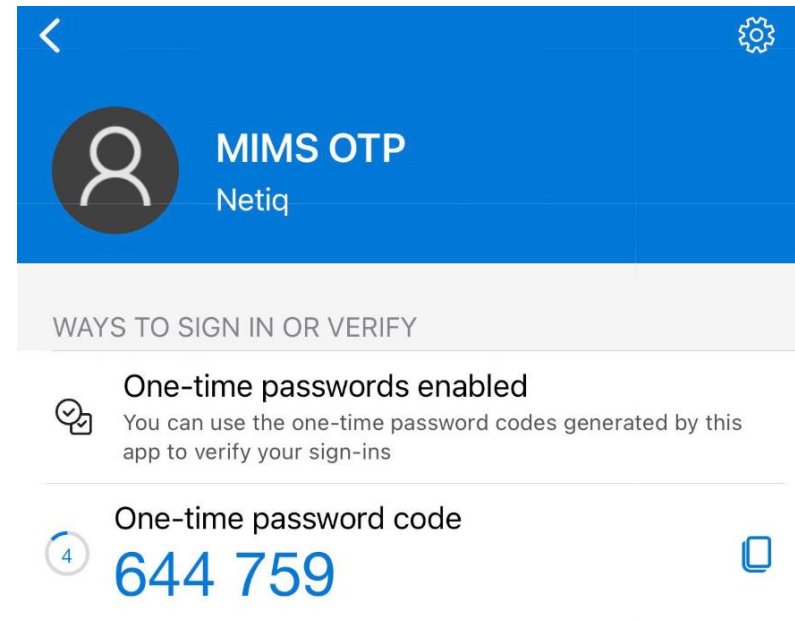
Upon successful login, you will see summary page as below:



2. Soft Token (OTP)

Mobile Token Enrolment

- Pre-requisite: Please ensure you have the following mobile authenticator installed in your mobile phone.
 - Microsoft Authenticator ([Guide](#))



Soft Token (OTP) Enrolment

Step 1: From the summary page, under Your Enrolled Single Methods for sign in, click on “Add”

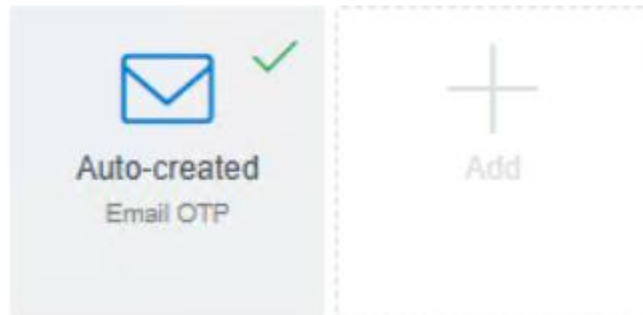
Welcome to the self-service portal for Advanced Authentication

This portal allows you to manage your authentication methods.

Enrolled methods are authenticators that you have already enrolled and can be used to sign in.
OTP methods are one-time password authenticators.

Your Enrolled Single Methods for sign in

This section displays all the methods that you have enrolled. You can click the add button "+" to add more.



Mobile Token Enrolment

Step 2: Select the Option "Soft Token (OTP)"

Available Methods for Enrollment

Select an authentication method for enrollment. Once enrolled, the method can be used for sign in. OTP methods are one-time password authenticators.



FIDO2



Soft Token (OTP)

Mobile Token Enrolment

Soft Token (OTP)

The Time-Based One-Time Password (TOTP) method generates a sequence of numbers called an OTP. This OTP must be used within a specified timeframe.

Display Name

My Soft Token (OTP)

Service Name

Account Name

Enroll this method using one of the following:

- In the OATH Token section, specify the OATH Token Serial Number, which is usually found on the back of the token. Generate and specify an OTP from the token.
- Click Get QR Code, then scan the QR code using a smartphone app.

OATH Token

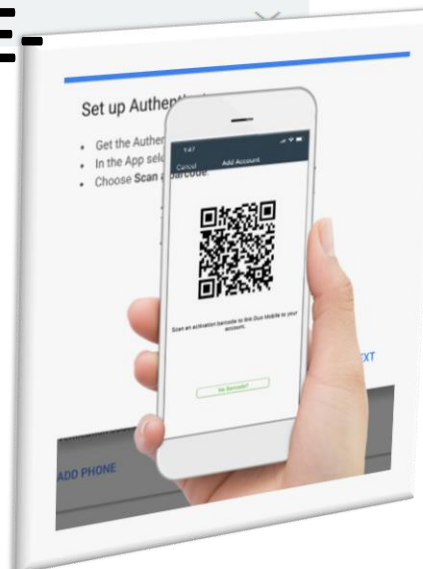
Get QR Code



Save

Cancel

-SAMPLE-

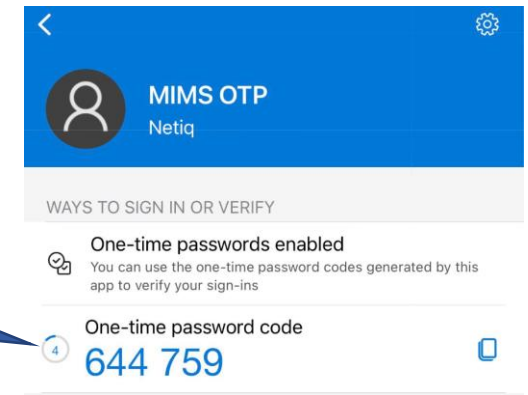


Step 3: Click on "Get QR Code" to display the QR code.

Step 4 In your smartphone, launch your mobile authenticator and scan the QR code to create a new mobile token.

Step 5: After scanning the QR code, click "Save".

Tips: Please ensure the OTP is valid by refer to the time bar



Mobile Token Enrolment

Upon successful setting up the Soft Token (OTP), you will see “My Soft Token (OTP)” under Your Enrolled Single Methods for sign in :

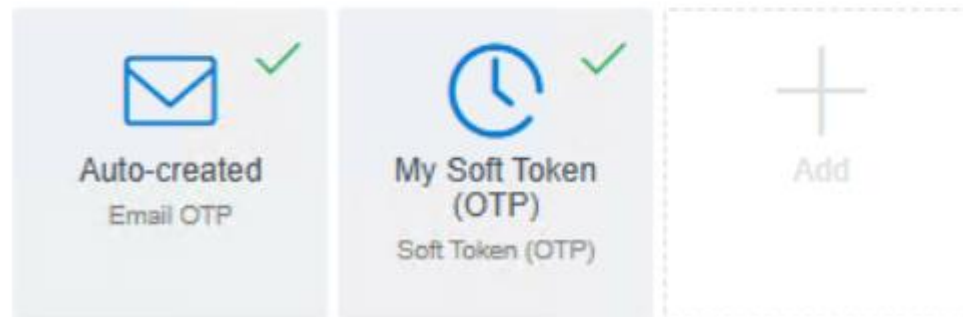
Welcome to the self-service portal for Advanced Authentication

This portal allows you to manage your authentication methods.

Enrolled methods are authenticators that you have already enrolled and can be used to sign in.
OTP methods are one-time password authenticators.

Your Enrolled Single Methods for sign in

This section displays all the methods that you have enrolled. You can click the add button "+" to add more.



Test on Enrolled Mobile Token

Step 1: Click on “My SoftToken (OTP)”

Step 2: Click on “Test Method” button to test the mobile token.

 Soft Token (OTP) ✓ 

The Time-Based One-Time Password (TOTP) method generates a sequence of numbers called an OTP. This OTP must be used within a specified timeframe.

Display Name

My Soft Token (OTP)

Test Method

Save

Cancel

Test on Enrolled Mobile Token

- Step 3 : Enter the generated OTP from the mobile authenticator and click "Test"
- Step 4: Click “Next” button to test the token.
- Refer to top right corner of the page to know if the test passed or failed.

The image displays three screenshots of a software interface for testing a soft token (OTP) method.

The top screenshot shows a dialog box titled "TEST SOFT TOKEN (OTP) METHOD" with a close button (X) in the top right corner. Below the title is a text input field labeled "Password" with a lock icon to its right. A yellow circle highlights a "Test" button located below the input field.

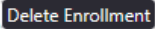
The bottom-left screenshot shows a smaller dialog box titled "TEST SOFT TOKEN (OTP) METHOD" with a close button (X) in the top right corner. It displays a green checkmark icon followed by the text "Test successful". Below this message is an "OK" button.

The bottom-right screenshot shows a smaller dialog box titled "TEST SOFT TOKEN (OTP) METHOD" with a close button (X) in the top right corner. It displays a red X icon followed by the text "Incorrect OTP". Below this message is an "OK" button.

Deleted Enrolled Mobile Token

- Step 1: Click on the 
- Step 2: Click “OK” button to delete the token
- Step 3: In your smart phone, remove the account from your authenticator apps

 Soft Token (OTP)  

The Time-Based One-Time Password (TOTP)  generates a sequence of numbers called an OTP. This OTP must be used within a specified timeframe.

Display Name

DELETE AUTHENTICATOR



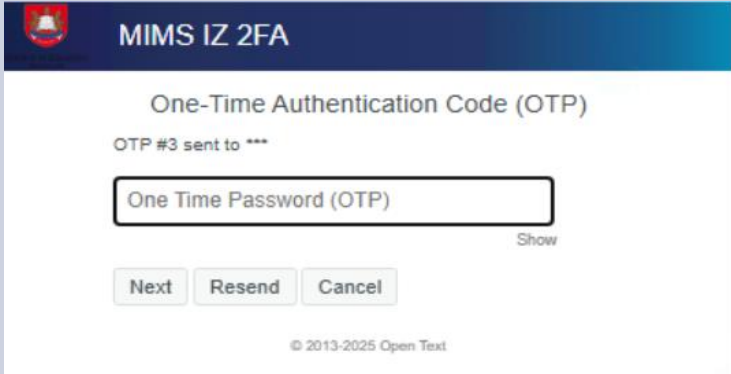
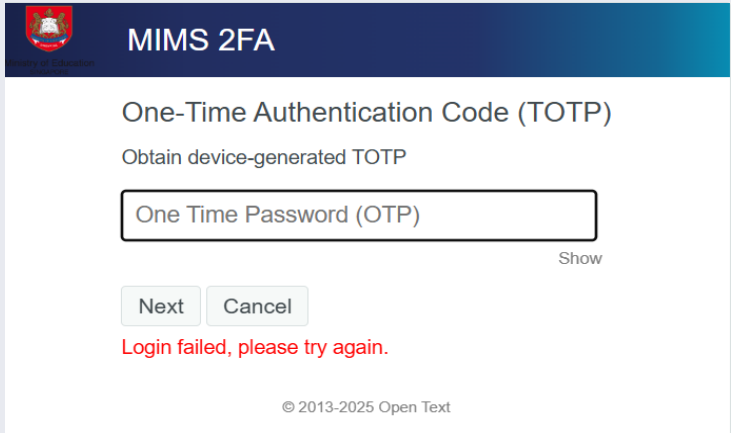
Are you sure you want to delete this authenticator?

OK

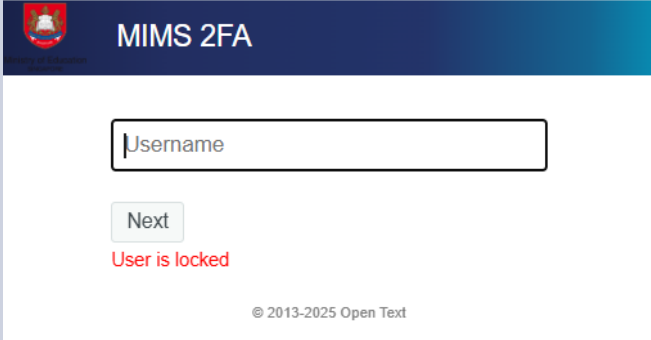
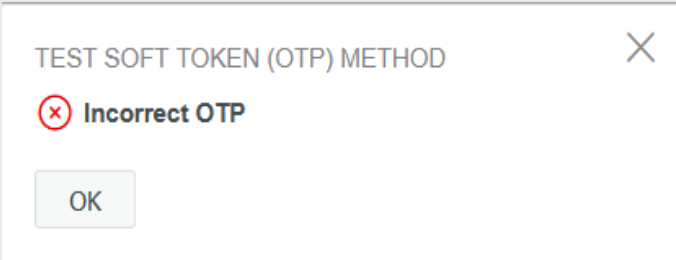
Cancel

3. FAQ

2nd Factor Authentication (2FA) FAQ

S/N	Questions	Answers
1.	The user did not receive the email OTP and encountered the message 'OTP # sent to ***'.  The screenshot shows the 'MIMS IZ 2FA' login interface. It features a header with the MIMS logo and the title 'MIMS IZ 2FA'. Below the header, the text 'One-Time Authentication Code (OTP)' is displayed. Underneath, it says 'OTP #3 sent to ***'. There is a text input field labeled 'One Time Password (OTP)' with a 'Show' button to its right. At the bottom, there are three buttons: 'Next', 'Resend', and 'Cancel'. The footer indicates '© 2013-2025 Open Text'.	User did not receive the email OTP due to the entry of an incorrect username (MIMS login ID). Please ensure that the user inputs the correct MIMS login ID, and the email OTP will be sent to their primary MIMS email address.
2.	The user encountered the error message 'Login failed, please try again'.  The screenshot shows the 'MIMS 2FA' login interface. It features a header with the MIMS logo and the title 'MIMS 2FA'. Below the header, the text 'One-Time Authentication Code (TOTP)' is displayed. Underneath, it says 'Obtain device-generated TOTP'. There is a text input field labeled 'One Time Password (OTP)' with a 'Show' button to its right. At the bottom, there are two buttons: 'Next' and 'Cancel'. Below the buttons, the error message 'Login failed, please try again.' is displayed in red. The footer indicates '© 2013-2025 Open Text'.	The user encountered this error due to the entry of an incorrect OTP. The user needs to 'Delete' the enrolled registered Soft Token OTP and then re-enroll. Please ensure that the device's timing is synchronized, including the date and time on both the device used to access the MIMS browser and the mobile device where the authenticator app is installed.

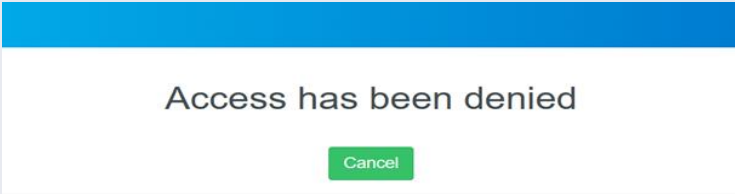
2nd Factor Authentication (2FA) FAQ

S/N	Questions	Answers
3.	The user encountered the 'User is locked' error after entering an incorrect OTP more than three times. 	Error: “User is locked” This message indicates that the user’s MFA is temporarily locked. Please wait 10–15 minutes for it to unlock automatically, then try again. If the issue persists, please delete and re-register the Soft Token (OTP).
4.	The user encounter 'Incorrect OTP' when performing "Test on Enrolled Mobile Token " 	This error is caused by the entry of an incorrect OTP. Even after deleting and re-enrolling, the user continues to encounter the same issue. Please ensure that the device's timing is synchronized, including the date and time on both the device used to access the MIMS browser and the mobile device where the authenticator app is installed. If the user is accessing multiple MIMS accounts, please ensure that each account has its own separate OTP enrolled in the authenticator app."

2nd Factor Authentication (2FA) FAQ

S/N	Questions	Answers
5.	If you encounter OTP validation problems when logging into applications like ICON using MFA.	Please follow these steps: 1. Log in to the Authentication Portal. Go to auth.mims.moe.gov.sg and sign in. 2. Remove Existing Soft OTP MFA Method. In the portal, delete the current soft OTP MFA method linked to your account. 3. Remove Existing Soft OTP from Your Smartphone. Open your authenticator app (Google Authenticator, Microsoft Authenticator, etc.) and delete the related OTP entry. 4. Re-enroll the Soft OTP MFA Method a. In the authentication portal, click the + sign to add a new soft OTP method. b. Scan the displayed QR code with your authenticator app on your smartphone. c. Click the Save button to confirm the new setup. 5. Test the newly Enrolled Soft OTP a. Select the newly added Soft OTP method in the portal. b. Click the “Test Method” button. c. Open your authenticator app and wait for a new OTP code to generate. d. Enter the the OTP code from your smartphone into the portal, wait for 20 seconds and click “Test” button. e. Verify that you see a Test Successful message. 6. Login to the Application Use the newly generated OTP from your authenticator app when prompted during MFA validation in the application (e.g., ICON).

2nd Factor Authentication (2FA) FAQ

S/N	Questions	Answers
6.	I just changed my device or mobile phone, and my existing MIMS 2FA setup no longer works. What should I do?	You will need to re-register 2FA on the new device to regain access. Please follow this steps : 1. Delete the currently enrolled soft token from MIMS. 2. Re-enroll the soft token on the new device. 3. Ensure the previously enrolled OTP is also removed from their mobile authenticator. 4. Add back the Soft Token (OTP). Please refer to page 15.
7.	Unable to set up MIMS 2FA. Encountered 'Access has been denied' after entering MIMS login ID. 	Please verify whether the email address has been updated in MIMS. If it has not, request the Local Administrator (LA) to update the email address in MIMS.

Thank you

