Science Tokyo ID
Initial Setup Manual
(Medical and Dental Sciences field)

Institute of
SCIENCE TOKYO

2025.4

IT Help Desk

Table of Contents

1. Confirmation of Science Tokyo ID Notification（Required）

About Science Tokyo ID

Science Tokyo has added a new authentication system, the Science Tokyo Authentication System.
The services available are different from those of the old authentication system (Tougou-ID),
so please be sure to make the initial settings for both upon receipt.

About Science Tokyo Gmail

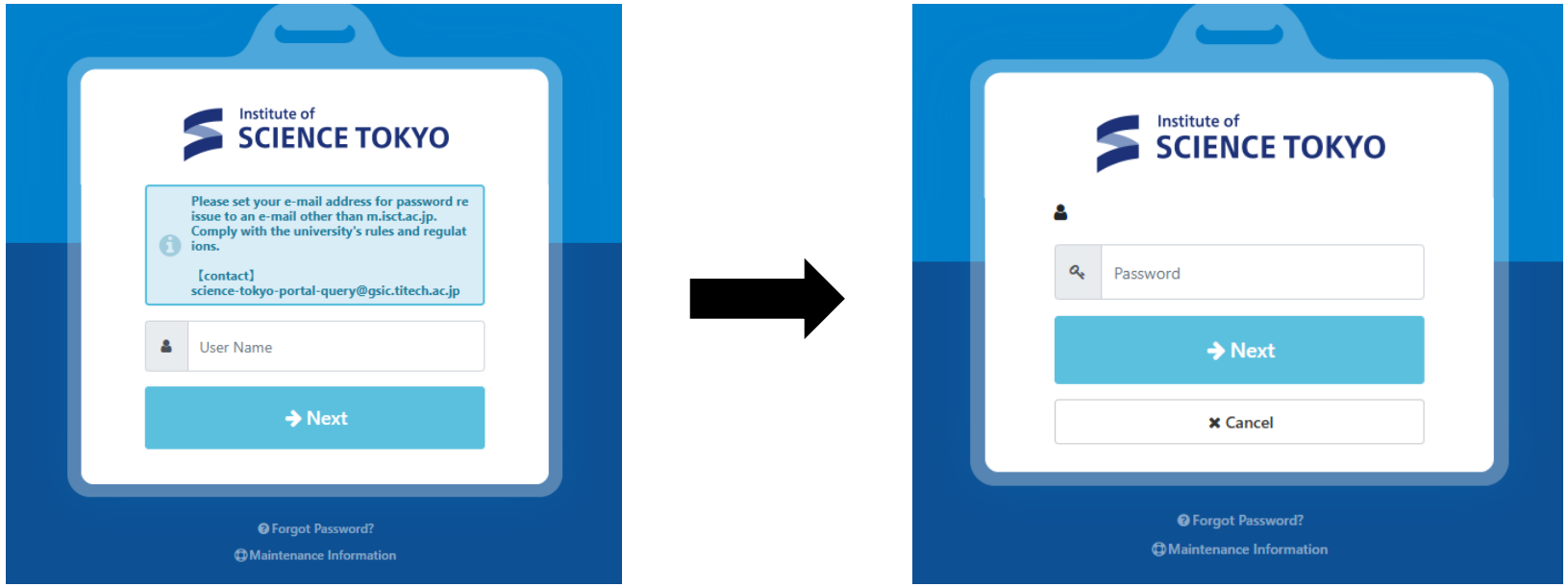
For information about Science Tokyo Gmail, please refer to the Science Tokyo Gmail webpage.

How to confirm your ID and initial password

URL for receiving Science Tokyo ID notification will be sent to TMDU email (@tmd.ac.jp)
for those who have a Tougou-ID and a Campus LAN Account.

2. Password Setup（Required）

Access to Science Tokyo portal

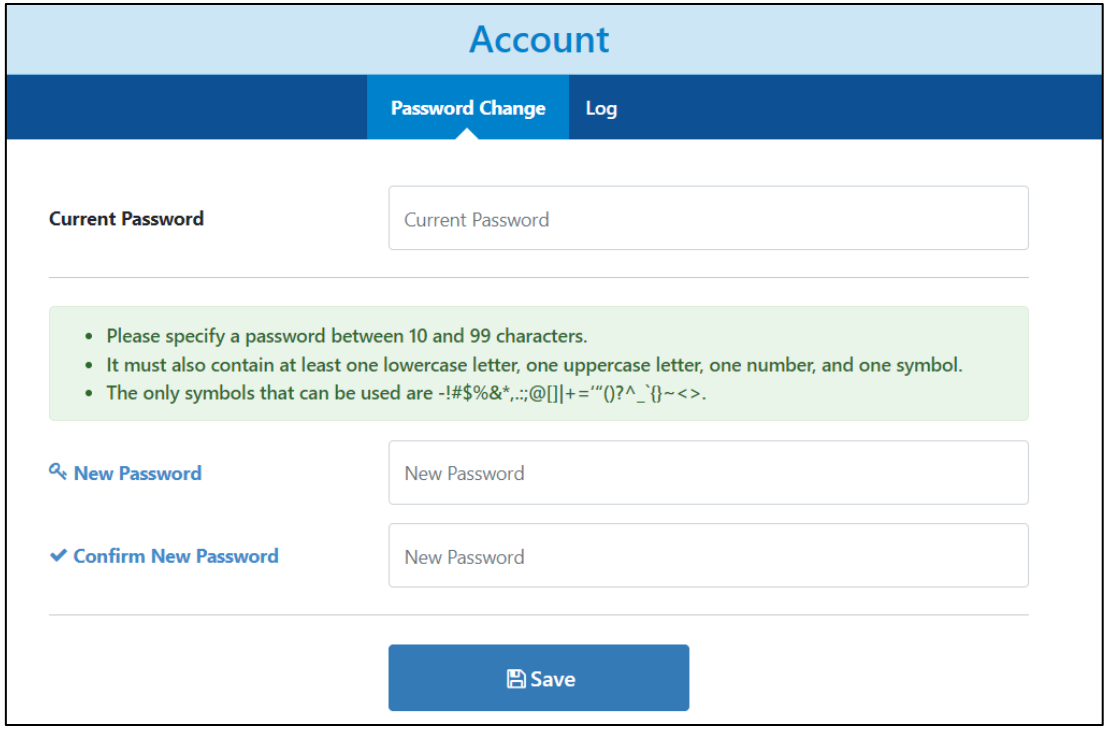


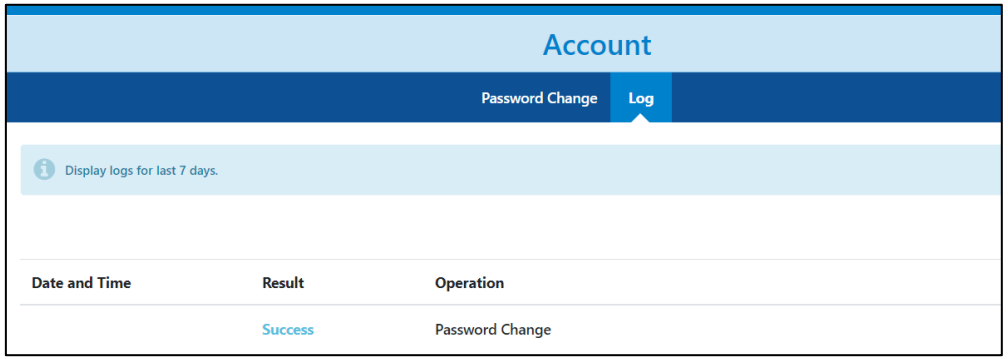
・In the "User Name" field, please enter your Science Tokyo ID.
This consists of four lowercase letters followed by four digits (a total of eight characters).

・Please enter the initial password you received in the “Password” field and click the "Next" button.

2. Password Setup（Required）

Set new password





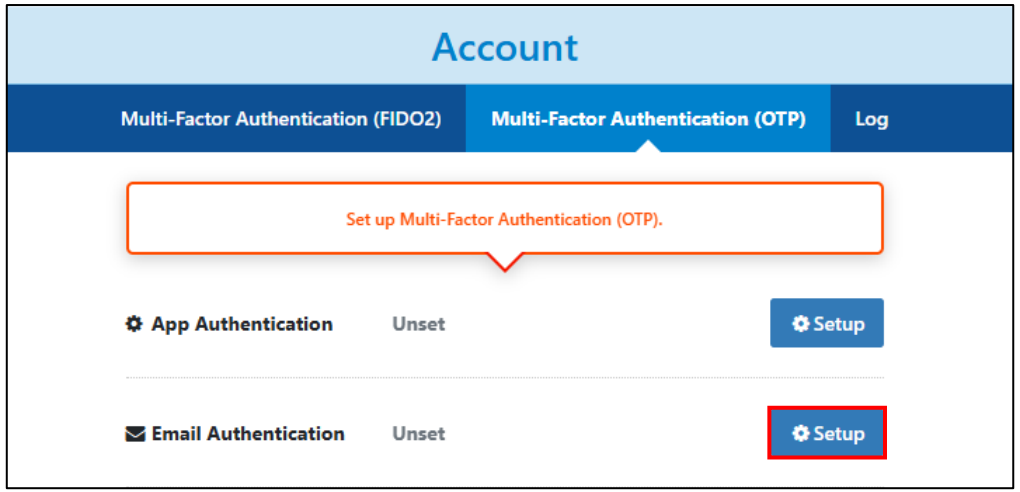
The "Password Change" will be recorded in the "Log".
※The "Result" is shown as "In Progress," but after a while, it will be updated to "Success."
There is no need to wait until it becomes "Success."

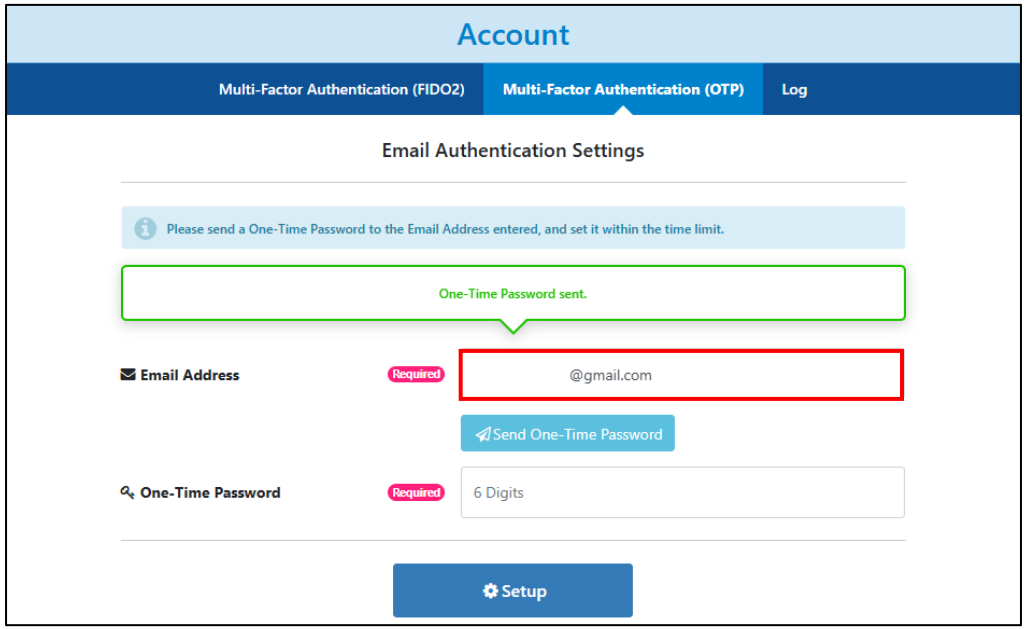
・In the "Current Password" field, please enter the initial password, then enter the password that meets the requirements in the "New Password“ and “Confirm New Password“ field, and click the "Save" button.

・Please specify a password between 10 and 99 characters.
・It must also contain at least one lowercase letter, one uppercase letter, one number, and one symbol.
・The only symbols that can be used are -!#$%&*,.:;@[]|+=‘“()?^_`{}~<>.

3. Setup of Multi-Factor Authentication(Email) (Required)

Email authentication settings





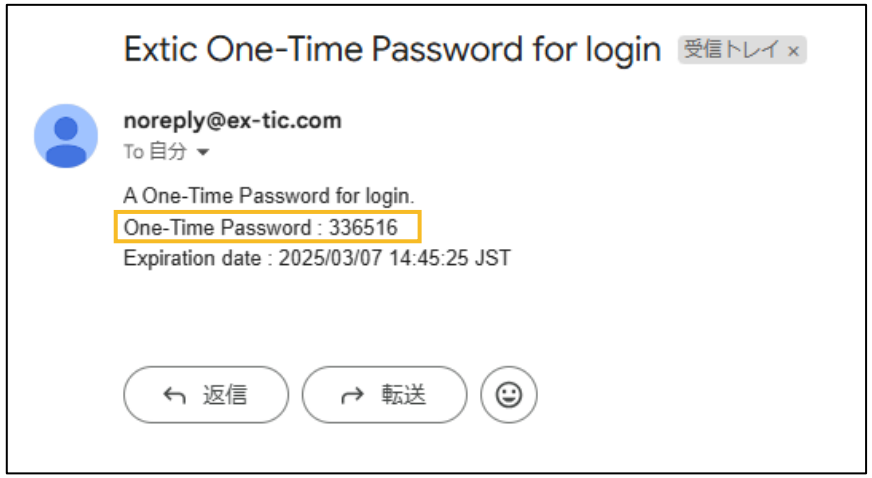
- Click on "Multi-Factor Authentication (OTP)" from the options in the top band, then click the "Setup" button at the right end of the "Email Authentication" row.

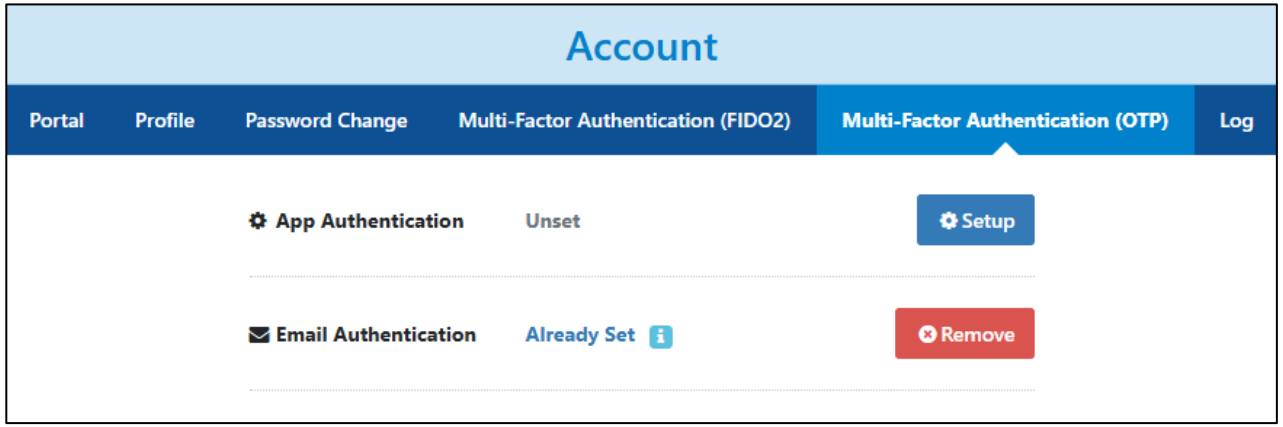
- Please enter the email address for receiving the one-time password in the "Email Address" field. After entering the email address, click the "Send One-Time Password" button.

Please use an email address that you can reliably check.
Science Tokyo email addresses (*@m.isct.ac.jp) and SaaS addresses (***@saas.isct.ac.jp) are not allowed.**
Carrier email addresses are not recommended.

3. Setup of Multi-Factor Authentication(Email) (Required)

Receiving the one-time password





When the setting is completed, “Email Authentication” under “Multi-factor Authentication (OTP)” will be marked as "Configured."

- A message containing the one-time password will be sent to the email address you entered.
  Please leave the window you are currently working on open as it is,
  and check the email contents in a different window or on another device.

- Enter the 6-digit One-Time Password from the e-mail in the “One-Time Password” field
  and press the “Setup” button.

4. Setup of Multi-Factor Authentication(App)

Institute of SCIENCE TOKYO

About App Authentication

With app authentication, you receive the one-time password (OTP) through an app instead of via email.
The app installed on your device (such as a smartphone or tablet) records a seed code,
which the app uses along with the current time to generate a one-time password.
Note: If the time of your device is incorrect, the one-time password will not be generated correctly.

The application is installed and set on your device.
If you change your device, you need to set it again on your new one.
※It cannot be set up on hospital smartphones.

Before starting to set up app authentication,
please install “**Google Authenticator**” from
the App Store (iOS) or Google Play Store (Android).

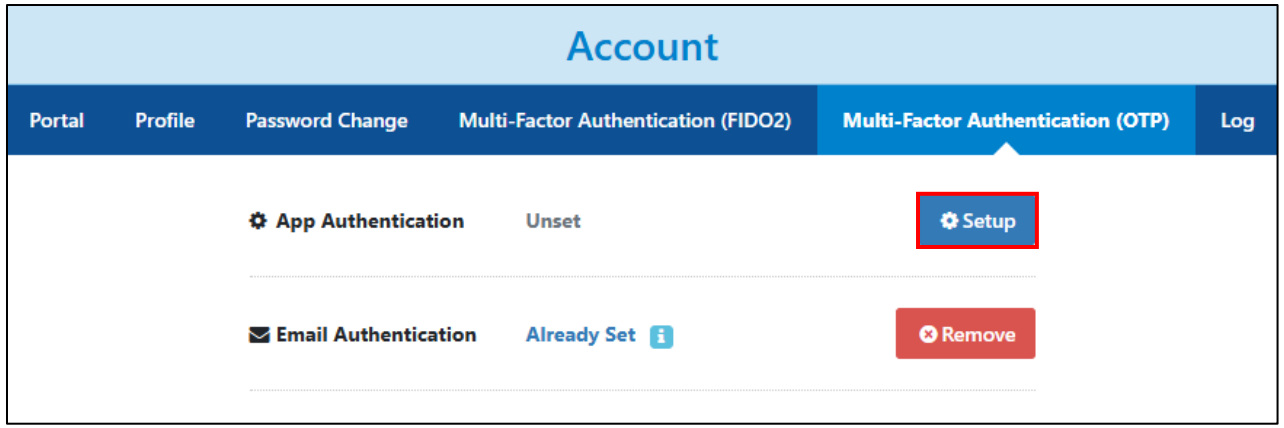
iOS

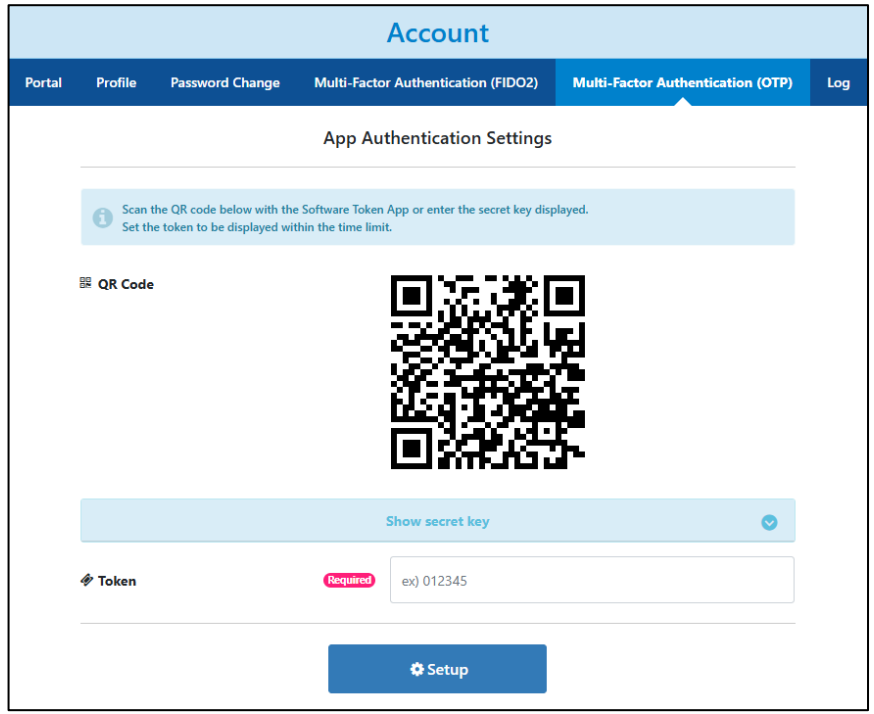
Android

4. Setup of Multi-Factor Authentication(App)

Institute of SCIENCE TOKYO

App authentication settings



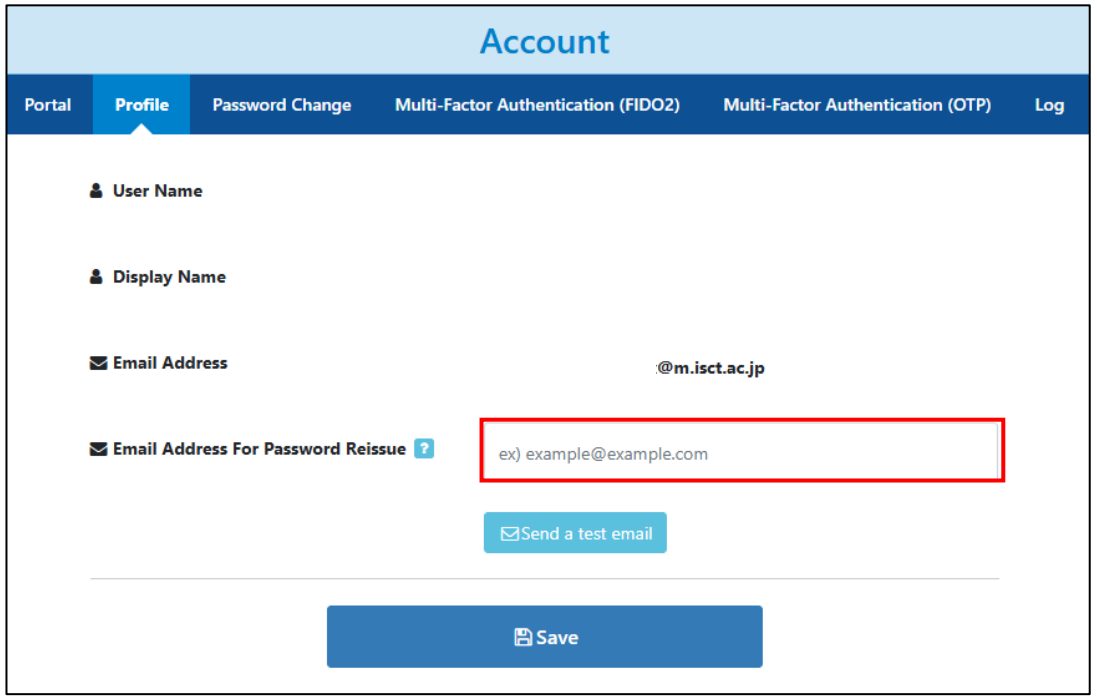


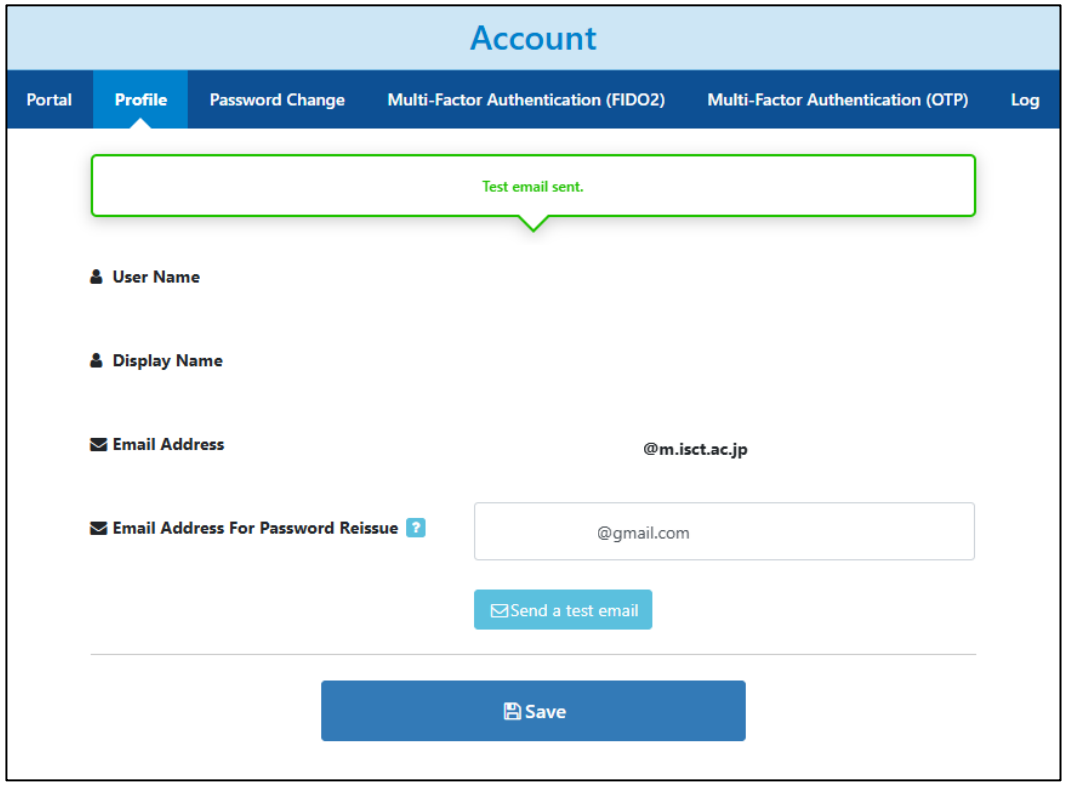
- Click on "Multi-Factor Authentication (OTP)" from the options in the top band, then click the "Setup" button at the right end of the “App Authentication" row.

- Scan the QR Code displayed on the screen with the “**Google Authenticator**” application. (※)
  Enter the token generated by the application in the “Token” field, and press the “Setup” button.

※For Google Authenticator, launch the app, press the “+” button at the bottom right of the screen, select “Scan a QR code,” and point the camera at the QR code. The necessary information will be entered into the app, and a six-digit number will be generated as a token.

5. Registration of Email Address for Password Reset (Required)





- Please click on "Profile" from the items in the top bar.

  Note: “Profile” will not appear unless at least one authentication setting has been completed.

  Please enter the email address for password reissue in the "Email Address For Password Reissue" field.

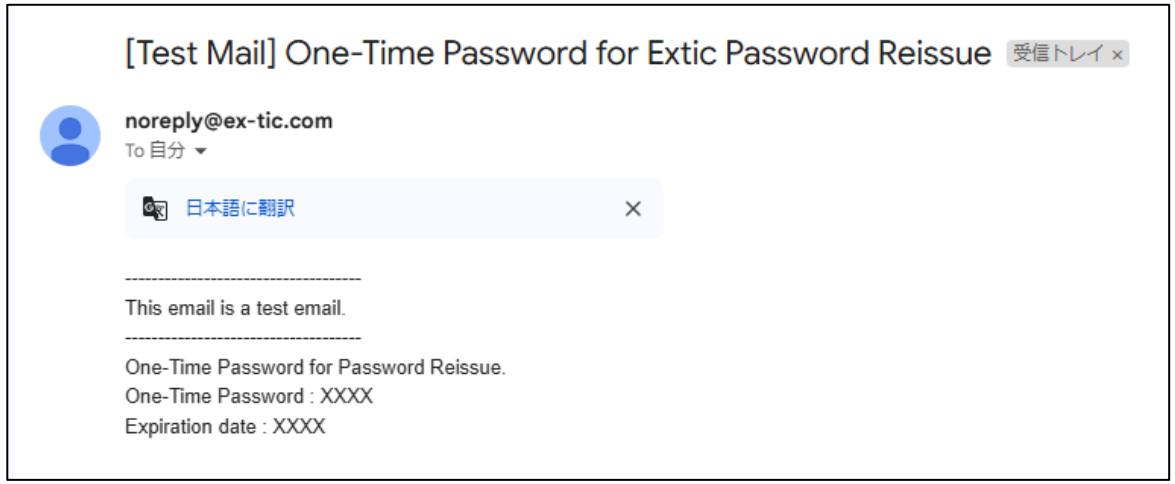
  After entering the email address, click the "Send a test email" button.

  ※ **You can use the same email address used to send the One-Time Passwords.**

  Science Tokyo email addresses (*@m.isct.ac.jp) and SaaS addresses (***@saas.isct.ac.jp) are not allowed.**

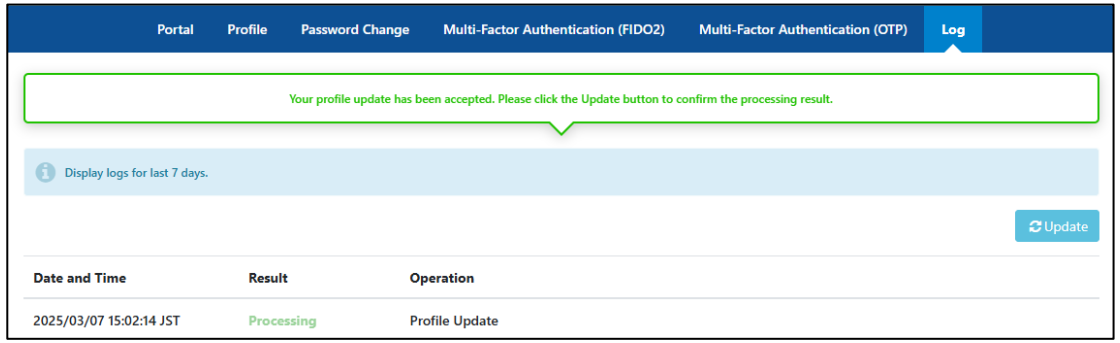
5. Registration of Email Address for Password Reset (Required)

Receive test email



≪If the email is not received≫
- **Check the email address again.**
- **Check your spam mailbox.**
- **Add domain “ex-tic.com” to filtering service in your provider.**
- **Try a different email address.**

・Confirm whether an email is received from the system at the email address you entered.
If the email is received, click the "Save" button.



When the setting is completed, “Profile Update” will be recorded in the “Log”.

6. Setup of Multi-Factor Authentication (FIDO2)

Institute of SCIENCE TOKYO

What is FIDO2 authentication

By setting up Multi-Factor Authentication (FIDO2), you can choose password-less authentication,
using mechanisms like fingerprint or facial recognition through the passkey system.
Note: Depending on the time of admission and entry into the program,
it may take some time before it becomes available for setting up.

Depending on the combination of your PC, authenticator, OS, and web browser,
FIDO2 authentication may not be possible.
Please ensure to perform a compatibility check before implementation.

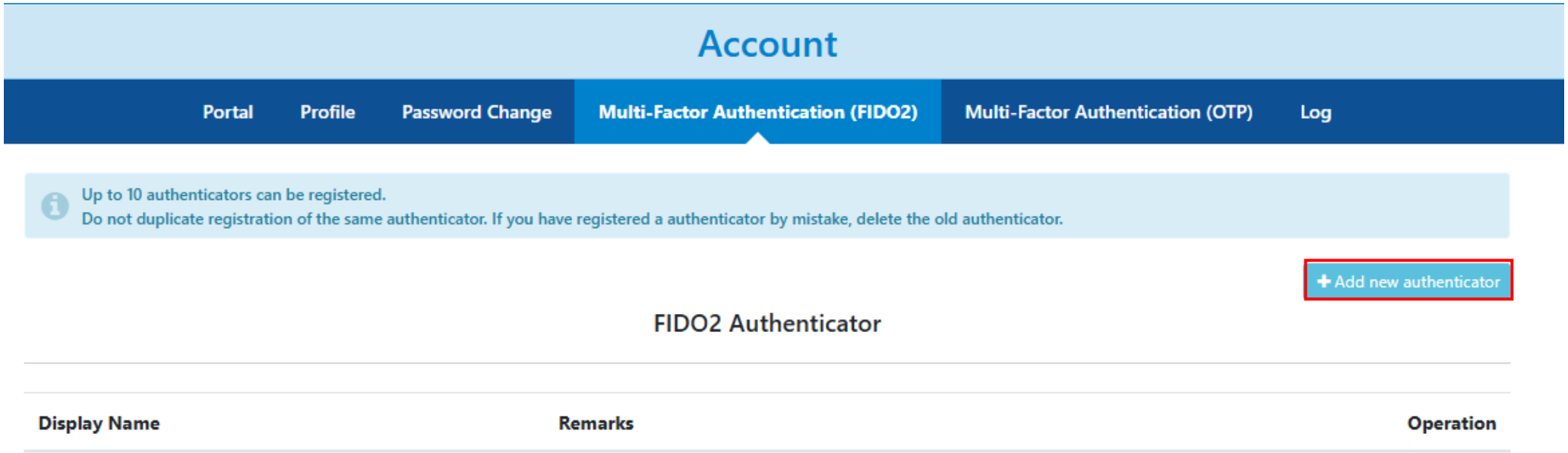
Information on "FIDO2 Compatible Authenticators" is available on the following website for your reference.
https://www.exgen.co.jp/extic/specs.html

6. Setup of Multi-Factor Authentication (FIDO2)

Institute of SCIENCE TOKYO

Setting Up FIDO2 authentication

Connect your authenticator or use a device with an integrated authenticator,
and login to Science Tokyo portal.
Select the「Multi-Factor Authentication (FIDO2)」tab → Click on 「Add new authenticator」

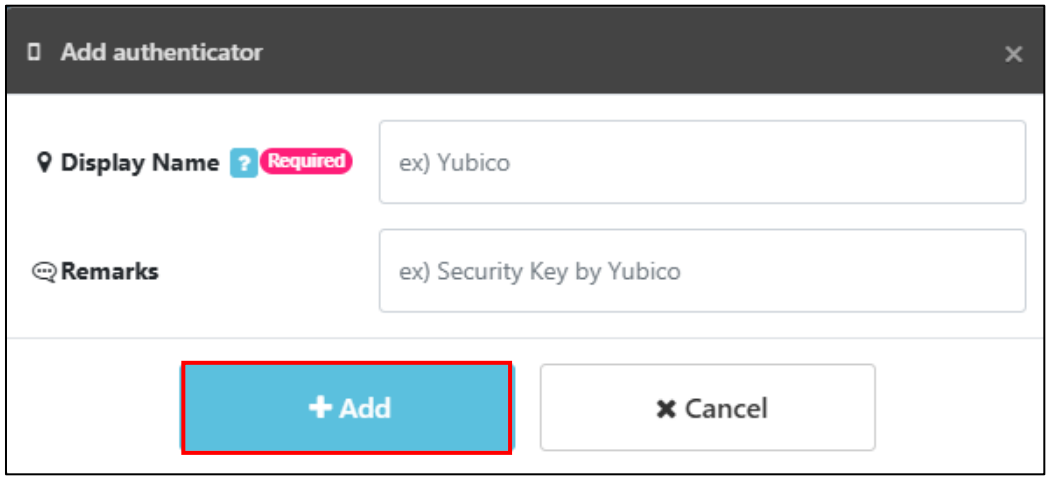


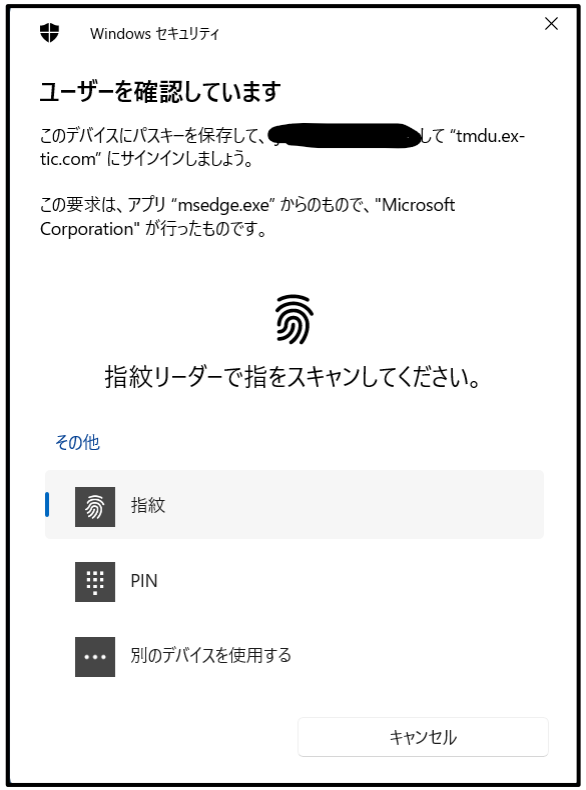
6. Setup of Multi-Factor Authentication (FIDO2)

Institute of SCIENCE TOKYO

Add an authenticator

・Enter a Display Name and click「Add」.





・Select your authenticator and authenticate.

・Click「OK」when the saved passkey appears.
If the authenticator has been added, the setup is complete.

※Authentication method varies depending on your authenticator.
※Devices already set up for Windows Hello, etc., may transition to authenticate.

7. How to log in after initial setup

Access to Science Tokyo portal

In the "User Name" field, please enter your Science Tokyo ID.

If you have not set up password-less authentication (①), or if you have set up password-less authentication but wish to authenticate using OTP (②), please enter the newly set password on the next screen.
※If ②, please select the password tab on the right side.

7. How to log in after initial setup

Multi-Factor Authentication (OTP) Email/App

Please enter your password in the “Password” field and click the "Next" button.

Up to three authentication methods will be displayed depending on the setting status of multi-factor authentication.
Please select “OTP(Email) Authentication” or “OTP(App) Authentication” and authenticate using OTP.

OTP(Email)

OTP(App)