

# **Logging into the Integrated Authentication System**

March 2026

ICT Office

---

# Contents

---

1. MFA for the Integrated Authentication System .....	3
2. Preparation.....	3
3. Login Procedure.....	4
3.1. For the First Login.....	4
3.2. After the First Time .....	8
3.3. When the Initial Configuration Fails to Load .....	9
3.4. Resetting the One-Time Code.....	13
4. Multi-factor Authentication Using Only a Smartphone.....	15
5. Other .....	19

---

---

At Sophia University, system logins are conducted via an Integrated Authentication System (Single Sign-On, hereafter referred to as SSO) that incorporates multi-factor authentication. Multi-factor authentication enhances security by requiring additional authentication information beyond just an ID and password. **It is necessary when accessing internal systems from external networks.**

Note: Multi-factor authentication is not required when using the campus network (such as sophiawifi2019).

As of February 2026, the systems that use the Integrated Authentication System include:

- Sophia Mail
- Loyola
- My Sophia
- Moodle
- CaLabo MX
- Self-Learning Portfolio
- My OPAC (Library OPAC)
- Mailing List System
- Zoom
- VPN
- Certificate Issuance System
- Career Center System
- Medical Checkup Results

As of February 2026, the individuals subject to multi-factor authentication (MFA) are as follows:

- Faculty and Staff
- Students (including those in Junior College Division)
- Professor Emeritus

# 1. MFA for the Integrated Authentication System

Starting August 29, 2025, Multi-Factor Authentication (MFA) has been implemented for logging into the Integrated Authentication System (Single Sign-On/SSO).

Multi-Factor Authentication enhances security by requiring additional authentication information beyond just an ID and password. Authentication is performed by entering the one-time code displayed in the dedicated app installed on the user's personal smartphone.

To enhance information security, multi-factor authentication was fully implemented on February 26, 2026.

The procedure for enabling multi-factor authentication is outlined below.

For instructions on how to log in using MFA after it has been configured, please refer to the section titled "Preparation".

## 2. Preparation

To log in to the integrated authentication system, a smartphone is required.

If you do not have a smartphone, please contact the ICT Office.

Please install the "Microsoft Authenticator" on your smartphone:



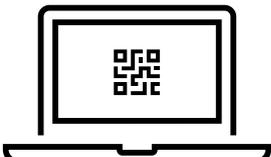
### 3. Login Procedure

#### 3.1. For the First Login

The following steps explain how to log in to the Integrated Authentication System for the first time after multi-factor authentication has been introduced.

For the initial setup, both a PC (to display the QR code) and a smartphone (to scan the QR code) must be prepared, as the QR code displayed on the screen needs to be scanned.

Required Items



Device to display the QR code  
(e.g., PC)



Device to scan the QR code  
(e.g., smartphone)

※As scanning the QR code is required, separate devices must be prepared for displaying and scanning.

- ① Access the ICT Office website at <https://ccweb.cc.sophia.ac.jp/en/> and click the system icon to log in. Loyola is used as an example here, but the process is the same for all systems.



- ② The integrated authentication login screen will appear. Enter your ID (faculty/staff number) and Sophia ICT account password.



- ③ A QR code will be displayed. At this point, **DO NOT scan the QR code with your smartphone's camera app.**

※The QR code is shown only during the first login. From the second login onward. Please refer to page 8. Section “3-2. After the First Time.

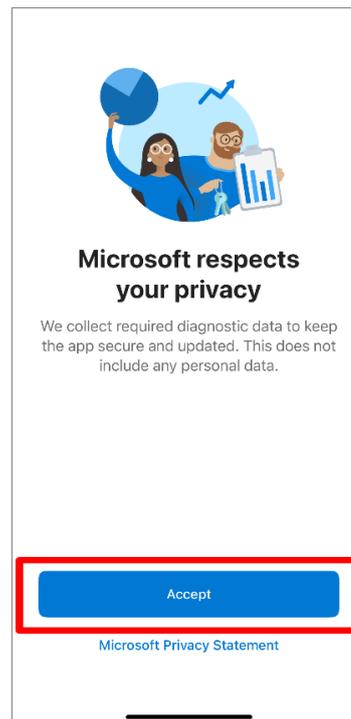
※If a new QR code is required, refer to page 13, **“3.4 Resetting the One-Time Code”.**



- ④ Launch the “Authenticator” app on your smartphone.



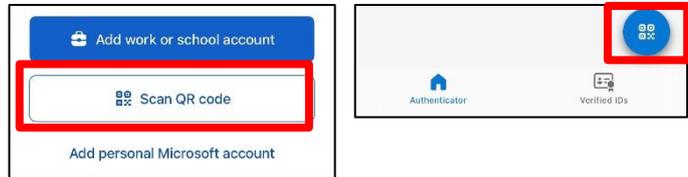
- ⑤ When the app opens, tap “Accept” on the screen.



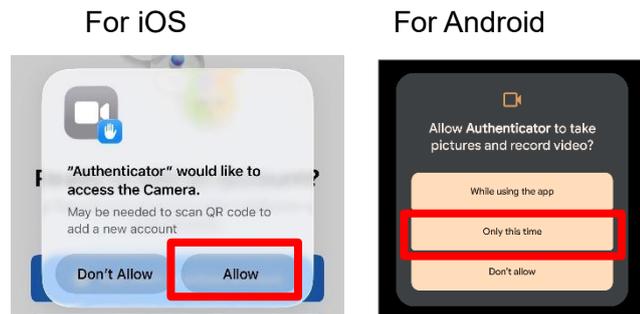
⑥ Tap “Continue”.



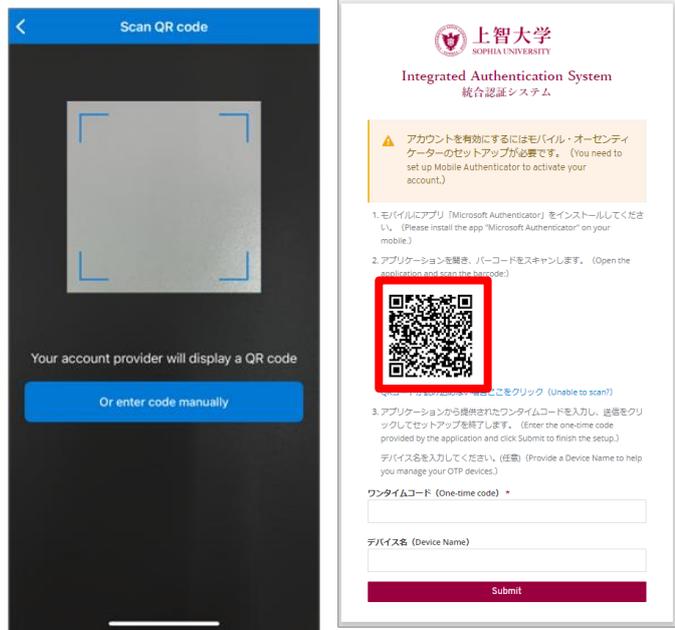
⑦ Tap “Scan a QR Code” or the QR code icon.



⑧ A message will appear asking for camera access. Select “Allow” or “Only this time”.

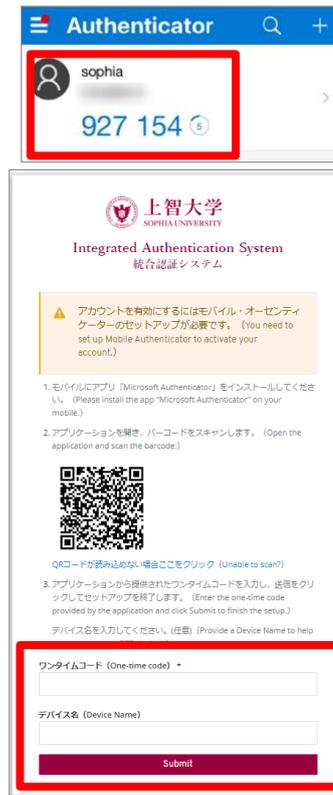


- ⑨ The QR code scanning screen will appear. Scan the QR code displayed on the Integrated Authentication System.

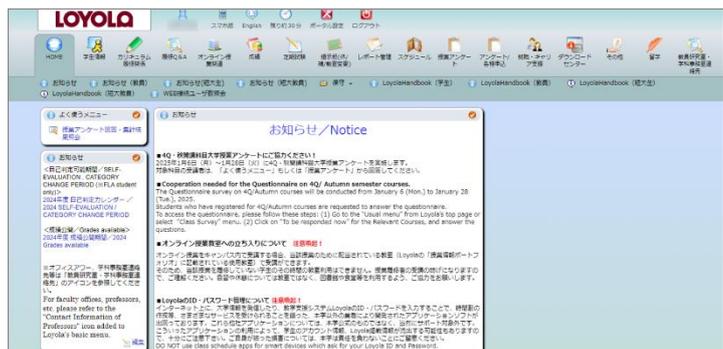


- ⑩ Once the QR code is scanned, a one-time code will appear under the “sophia” entry in the Microsoft Authenticator app. Enter this code in the “One-time code” field and tap “Submit”. Entering a device’s name is optional.

**\*No space between the two three-digit groups.**



- ⑪ Authentication is complete, and you will be logged into the system.



## 3.2. After the First Time

The following are the login steps for subsequent login.

- ① Access the ICT Office website at <https://ccweb.cc.sophia.ac.jp/en/> and click the system icon to log in. Loyola is used as an example here, but the process is the same for all systems.



- ② The Integrated Authentication Login screen will appear. Enter your ID (student/faculty number) and Sophia ICT account password.



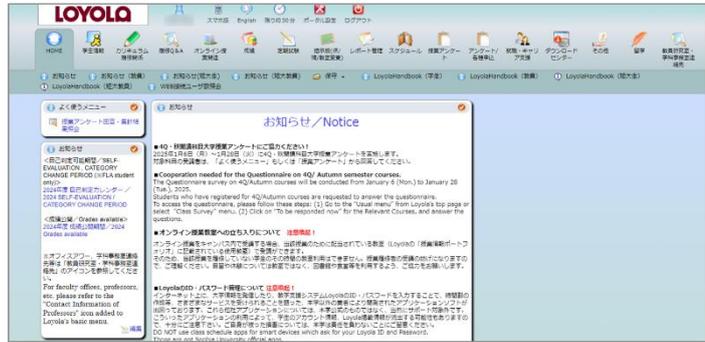
- ③ The screen for entering a one-time code will appear. Please open the Microsoft Authenticator app on your smartphone and check the code.



- ④ Enter the one-time code displayed in Microsoft Authenticator app into the "One-time code" field.  
**\*No space between the two three-digit groups.**



- ⑤ Authentication is complete, and you will be logged into the system.



### 3.3. When the Initial Configuration Fails to Load

- ① Using a different web browser from the one initially used (such as Safari or Google Chrome), or a new browser tab, access the ICT Office website (<https://ccweb.cc.sophia.ac.jp>) After selecting an application, the Integrated Authentication System login screen appears. Enter the ID (student/faculty number) and the password for the Sophia ICT account.



- ② A QR code will be displayed. At this point, please do not scan the QR code using your smartphone's camera app or any other scanning application.



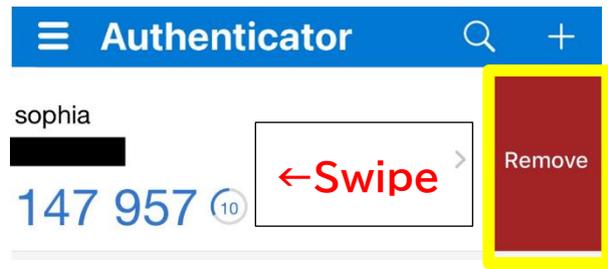
- ③ Please check your smartphone while leaving the computer screen as it is.

**First, delete the one-time code you initially scanned.**

(It is safe to delete any incorrectly displayed codes.)

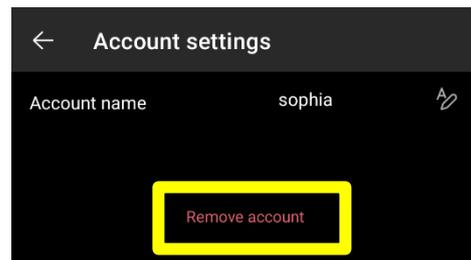
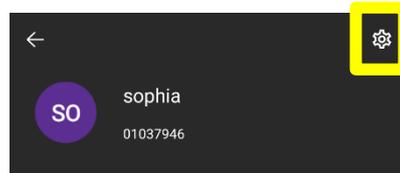
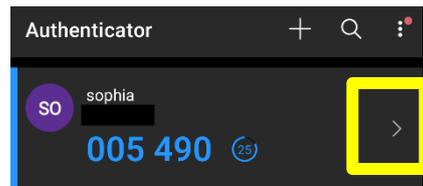
※For iPhone

1. Swipe the code that is displayed.
2. Tap 'Remove'.



※For Android

1. Tap the ">" icon.
2. Tap the gear icon.
3. Tap "Remove account".



- ④ Display the screen for scanning the QR code

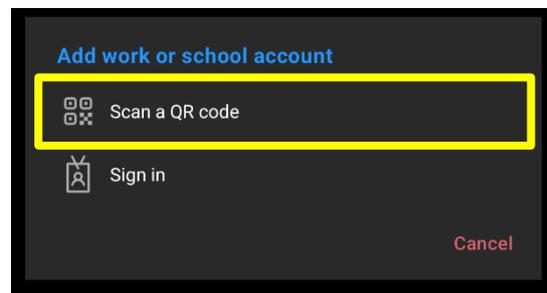
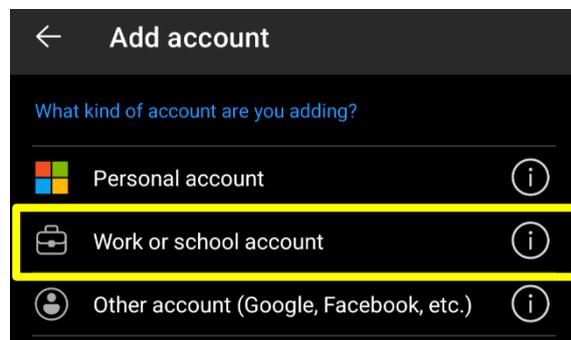
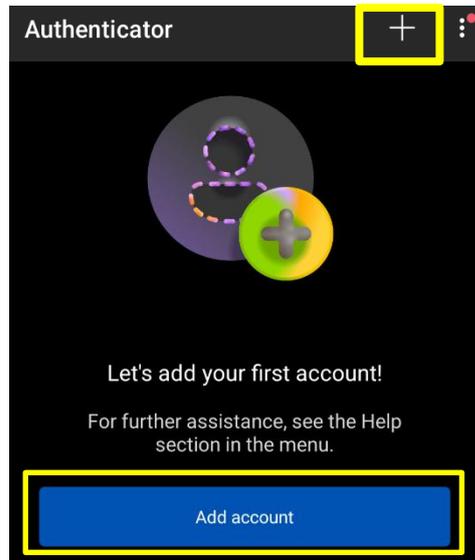
※For iPhone

Tap "Scan a QR code" or the QR Code icon.



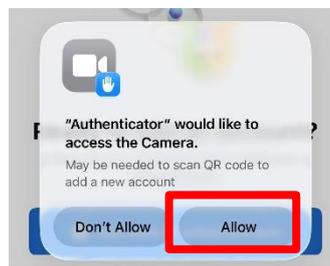
※For Android

1. Tap “Add account” or “+”.
2. Select “Work or school account”.
3. Select “Scan a QR code”.

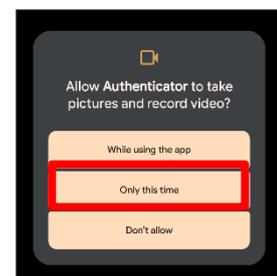


- ⑤ A message will appear asking for camera access. Select “Allow” or “Only this time”.

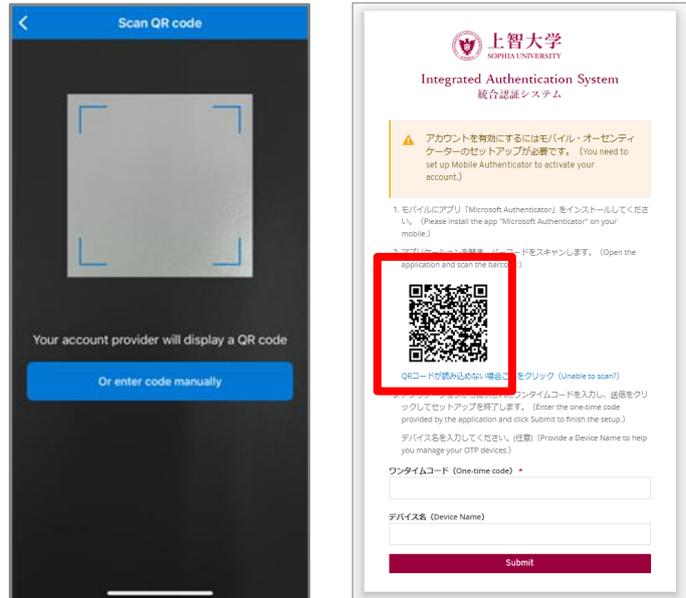
For iOS



For Android



- ⑥ The QR code scanning screen will appear. Scan the QR code displayed on the Integrated Authentication System.



- ⑦ Once the QR code is scanned, a one-time code will appear under the “sophia” entry in the Microsoft Authenticator app. Enter this code in the “One-time code” field and tap “Submit”. Entering a device’s name is optional.  
**\*No space between the two three-digit groups.**



## 3.4. Resetting the One-Time Code

Resetting the one-time code is required in the following cases:

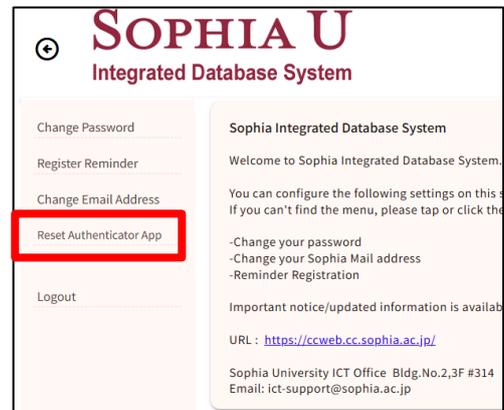
- Smartphone (device with the Microsoft Authenticator app installed) has been replaced
- Smartphone (Microsoft Authenticator app installed) has been lost
- Microsoft Authenticator app has been uninstalled
- Settings within the Microsoft Authenticator app have been deleted
- Reconfiguration of the one-time code is necessary for any other reason

① Log in to the Integrated Database.

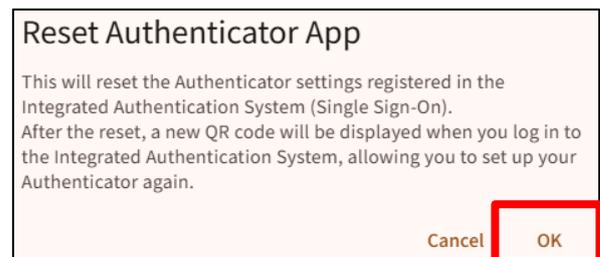
<https://idb.sophia.ac.jp/sophiaDBunion/en/login>

※If two-factor authentication for the Integrated Database has not been completed, complete the setup first by following the steps in “[this guide](#)”.

② Click “Reset Authenticator App”.

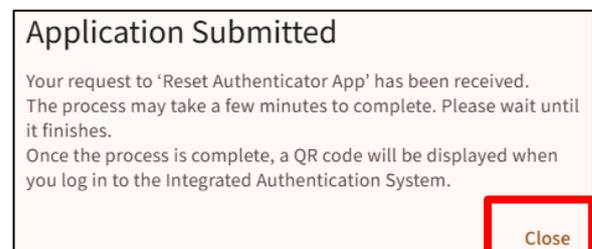


③ Click “OK”.



④ Click “Close”.

Please wait about five minutes for the process to complete before proceeding to the next step.



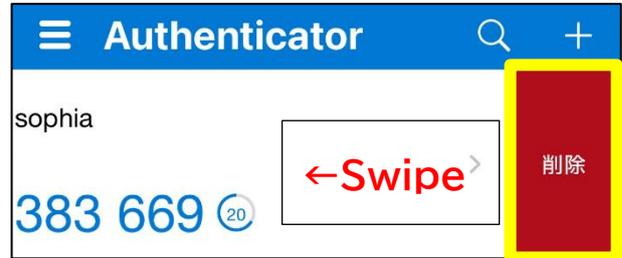
⑤ Return to [“3.1. For the First Login”](#) and complete the setup.

※If old settings remain in the Microsoft Authenticator app, delete them using the steps below.

(1) Open the “Authenticator” app on the smartphone.



(2) Delete the old settings.



(3) If a warning appears, click ‘Continue’.

## 4. Multi-factor Authentication Using Only a Smartphone

Although it is strongly recommended to complete the setup described in [“3.1 For the First Login”](#) the following method can be used when the setup cannot be performed due to circumstances such as only a smartphone being available.

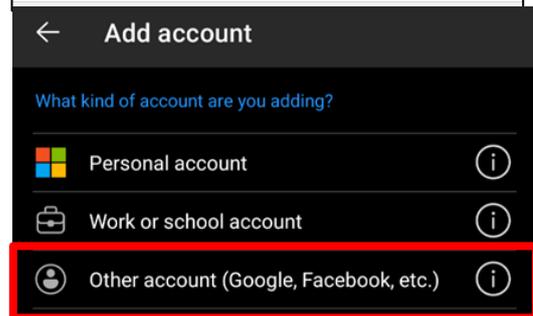
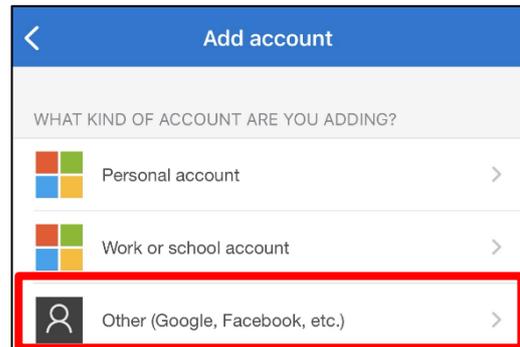
Please note that this method requires switching between applications on the smartphone during the setup process; the procedure is more difficult to complete.

- ① Launch the Authenticator app and tap [+] at the top of the screen.

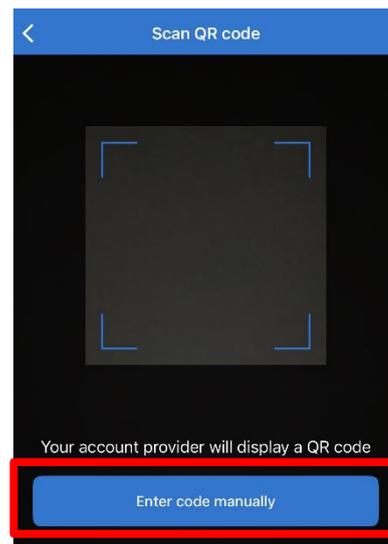


(Do not connect to “sophiawifi2019” at this time)

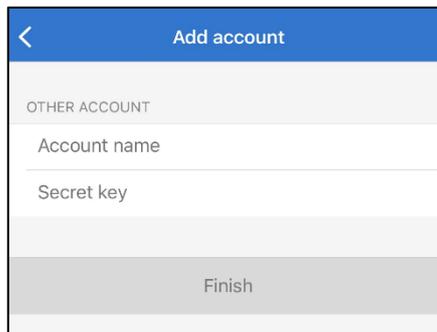
- ② Select [Other (Google, Facebook, etc.)] or [Other account (Google, Facebook, etc.)].



- ③ Select [Enter code manually].



- ④ The “Add account” screen will appear.



- ⑤ **Without closing the Authenticator screen,** access the ICT Office website at <https://ccweb.cc.sophia.ac.jp> and click the icon for the system to be logged into. In this manual, Loyola is used as an example, but the procedure is the same for any system.



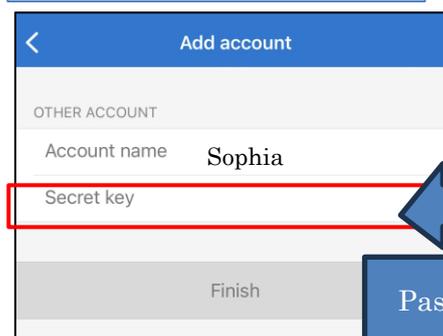
- ⑥ When the Integrated Authentication System login screen appears, enter the ID (student ID number or faculty/staff number) and the Sophia ICT account password.



- ⑦ Tap [Unable to scan?].



- ⑧ Copy the displayed key and paste it into the Secret key field in the Authenticator app. Enter “Sophia” or the student/faculty/staff number as the account name, and then tap “Finish”.

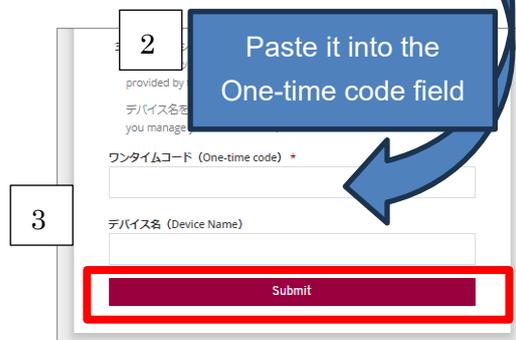


- ⑨ After completing the setup, an entry labeled “Sophia” or the student/faculty/staff number will appear in the Microsoft Authenticator app. Copy the displayed code and paste it into the “One-time code” field, then tap [Submit]. Entering a “Device Name” is optional.

※For iPhone

1. Tap the six-digit code to copy it.
2. Open the web browser and paste the code into the One-time code field.
3. Tap [Submit].

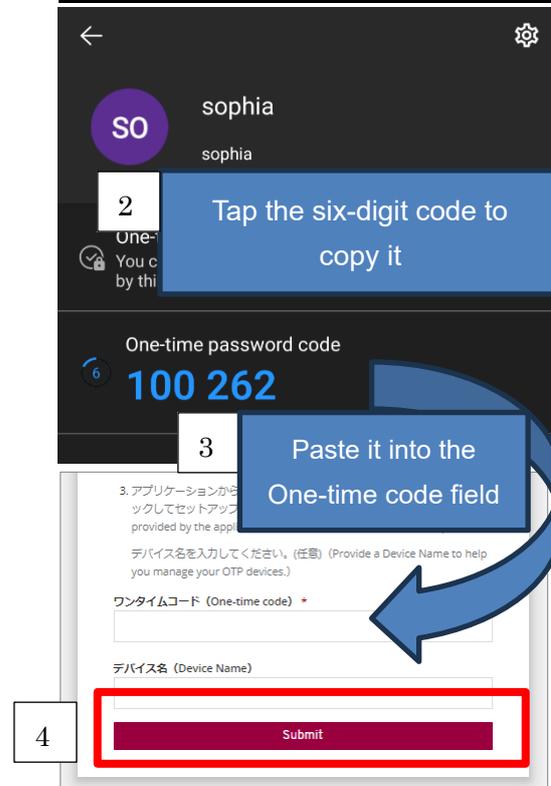
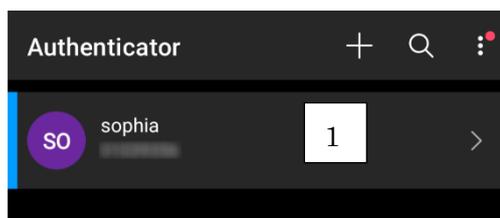
< For iPhone >



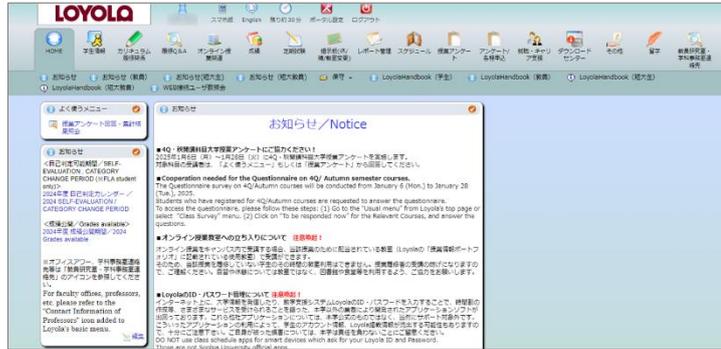
※For Android

1. Tap the entry labeled “sophia” or the student/faculty/staff number.
2. Tap the six-digit code to copy it.
3. Open the web browser and paste the code into the One-time code field.
4. Tap [Submit].

< For Android >



- ⑩ Authentication is now complete, and access to the system is available.  
For subsequent logins, please refer to [“3.2 After the First Time”](#).



## 5. Other

- In cases such as changing a smartphone model, losing a device, or accidentally uninstalling **Microsoft Authenticator**, a new QR code will be required. Please follow the instructions in [“3.4 Resetting the One-Time Code”](#) to complete the setup.
- If you do not have a smartphone, please contact the ICT Office by email.
- Regarding Multi-Factor Authentication applications other than Microsoft Authenticator, while the ICT Office does not provide support for them, you are free to use them (e.g., Google Authenticator, Duo Mobile).  
However, please note that the user must resolve any issues that arise during initial setup or use.
- If the QR code for the initial setup is scanned but the code is entered incorrectly even once, or if the setup screen is left open for an extended period, the QR code will be refreshed. If the message “Invalid code” continues to appear despite repeated attempts, please follow the instructions in [“3.3. When the Initial Configuration Fails to Load”](#) properly and perform the setup again.

## Logging into the Integrated Authentication System

August 2025 Created a new document.

September 2025 Revised.

November 2025 Revised.

December 2025 Revised.

December 2025 Revised.

January 2026 Revised.

February 2026 Revised.

March 2026 Revised.

Author Sophia University ICT-Office

Address 102-8554

Kioicho 7-1, Chiyoda-ku, Tokyo-to, Japan.

Phone 03(3238)3101

Website <http://ccweb.cc.sophia.ac.jp/>

**Sophia ICT**

Search

