

Logging into the Integrated Authentication System

January 2026

ICT Office

Contents

1. Enabling MFA for the Integrated Authentication System	3
2. Preparation.....	4
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.....	10
4. Other	14

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 January 2026, the systems that use the Integrated Authentication System include:

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

1. Enabling 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).

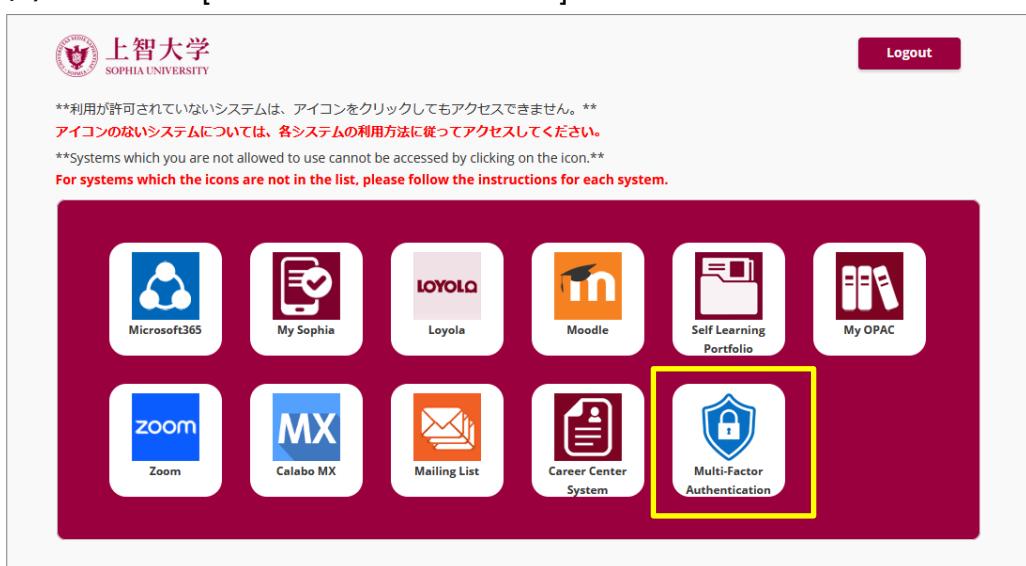
Multi-Factor Authentication enhances security by requiring additional authentication information beyond just an ID and password.

While MFA is optional at the time of introduction, it is scheduled to become mandatory early in the fall semester to enhance information security.

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".

- (1) Log in to the Integrated Authentication System (<https://sso.sophia.ac.jp>).
- (2) Click the [Multi-Factor Authentication] Icon.



- (3) Check the box labeled [Enable Multi-Factor Authentication].
Ensure that "Authenticator" is selected as the authentication method, then click [Save].



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:



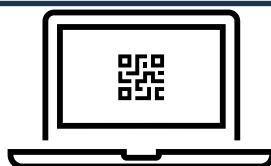
3. Login Procedure

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.

The screenshot shows a grid of icons representing different systems. The 'LOYOLA' icon, which is a red square with the word 'LOYOLA' in white, is highlighted with a red rectangular box. Other icons include 'PASSWORD・メールアドレス', 'Microsoft365 教職員ログイン', 'Microsoft365 学生ログイン', 'Moodle', 'Sophia Web Print(学内ネットワーク/VPN経由)', 'VPN', '開室カレンダー', '教室利用状況', and 'セルフ学修ポートフォリオ'.

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

The screenshot shows the 'Integrated Authentication System' login page. It features the Sophia University logo and the text 'Integrated Authentication System' and '統合認証システム'. Below the logo are two input fields: 'Login ID' and 'Password', which are highlighted with a red rectangular box. Below the fields is a link 'Click the link if you have forgotten your password.' and language options '日本語/English'. At the bottom is a large red 'Login' button.

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.”

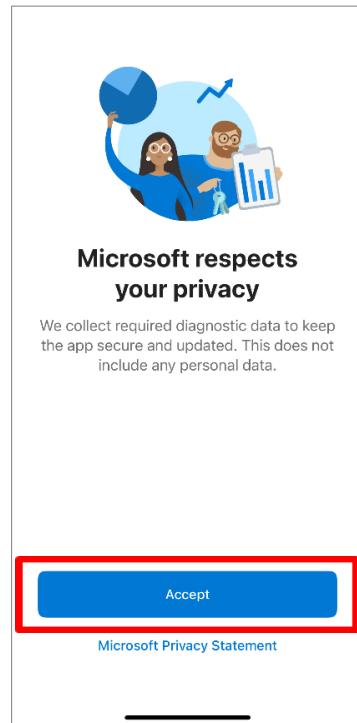
※In case you have uninstalled "Microsoft Authenticator" after setting up multi-factor authentication and need to reconfigure it, please see section 4 "Other" on page 14.

The screenshot shows the 'Integrated Authentication System' setup page for 'Microsoft Authenticator'. It features the Sophia University logo and the text 'Integrated Authentication System' and '統合認証システム'. A warning message in a yellow box states: 'アカウントを有効にするにはモバイル・オーセンティケーターのセットアップが必要です。 (You need to set up Mobile Authenticator to activate your account.)'. Below the message are two numbered steps: 1. 'モバイルにアプリ「Microsoft Authenticator」をインストールしてください。 (Please install the app "Microsoft Authenticator" on your mobile.)' and 2. 'アプリケーションを開き、バーコードをスキャンします。 (Open the application and scan the barcode.)'. A QR code is displayed for scanning. Below the QR code are instructions: 'QRコード読み込めない場合ここをクリック (Unable to scan?)', '3. アプリケーションから提供されたワンタイムコードを入力し、送信をクリックしてセッティングを完了します。 (Enter the one-time code provided by the application and click Submit to finish the setup.)', and 'デバイス名を入力してください。(任意) (Provide a Device Name to help you manage your OTP devices.)'. There are input fields for 'ワンタイムコード (One-time code)' and 'デバイス名 (Device Name)', and a red 'Submit' button.

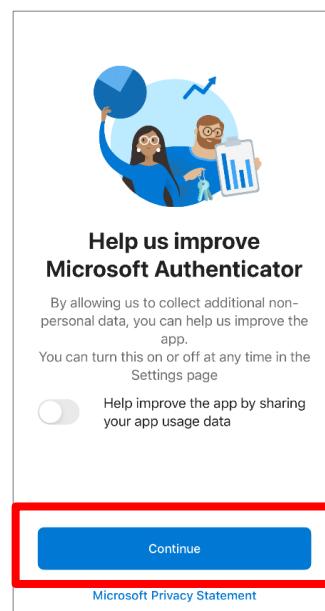
④ Launch the "Authenticator" app on your smartphone.



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



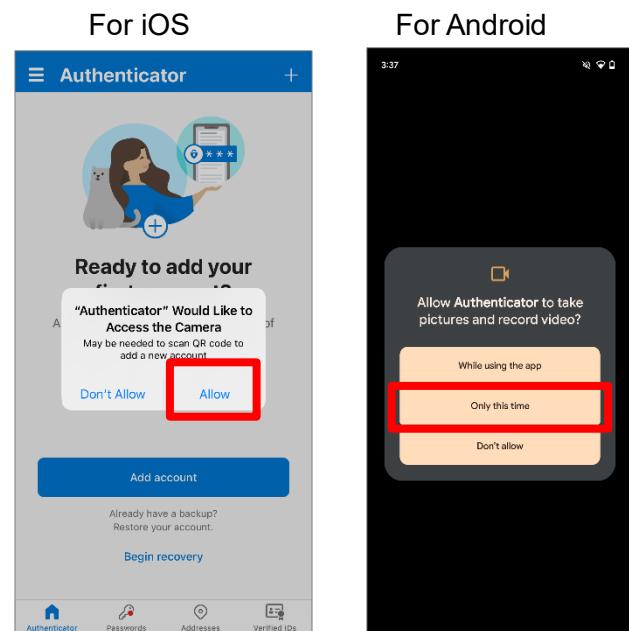
⑥ Tap “Continue”.



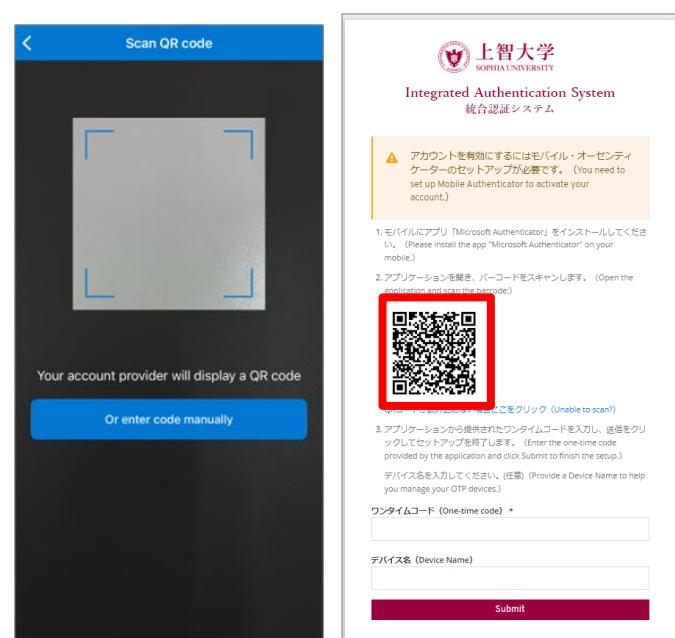
⑦ Tap “Scan a QR Code”.



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 Authentication 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 logins.

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.

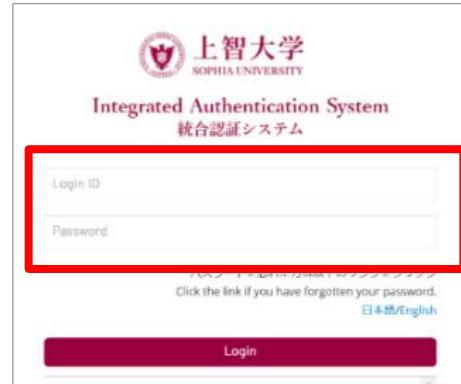


3.3. When the Initial Configuration Fails to Load

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.



The screenshot shows the 'Integrated Authentication System' login page. At the top is the Sophia University logo and name. Below it is a red box highlighting the 'Login ID' and 'Password' input fields. A link for password recovery and language selection ('日本語/English') are also visible.

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.



The screenshot shows the 'Mobile Authenticator' setup page. It includes a warning message about setting up the mobile authenticator, step-by-step instructions (install app, scan barcode), a QR code for scanning, and input fields for the one-time code and device name, followed by a 'Submit' button.

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

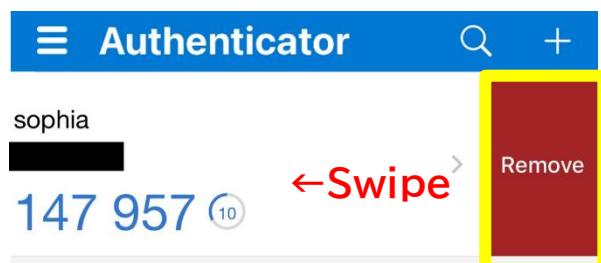
First, delete the one-time code you initially scanned.

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

※For iPhone

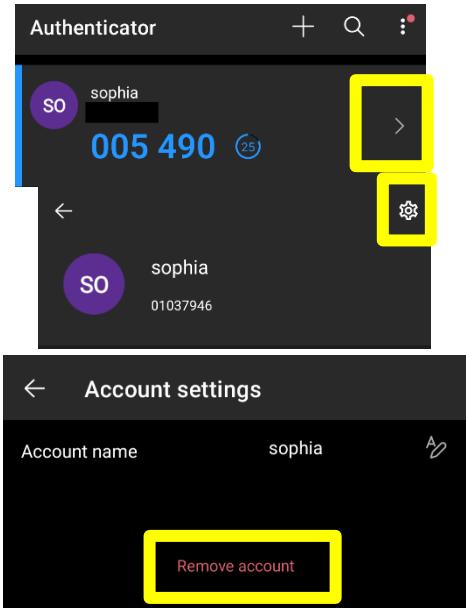
1. Swipe the code that is displayed.

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

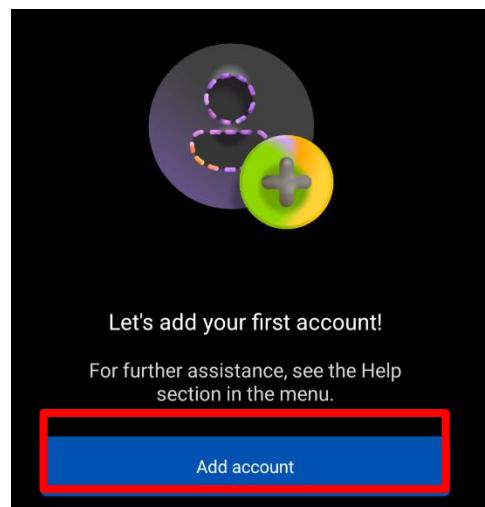
※For iPhone

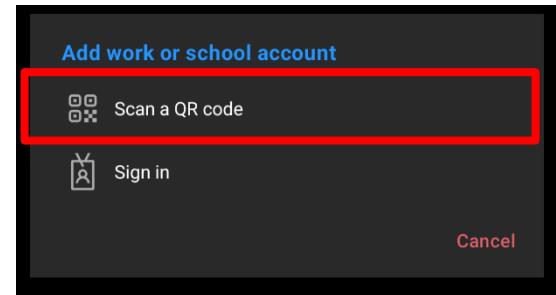
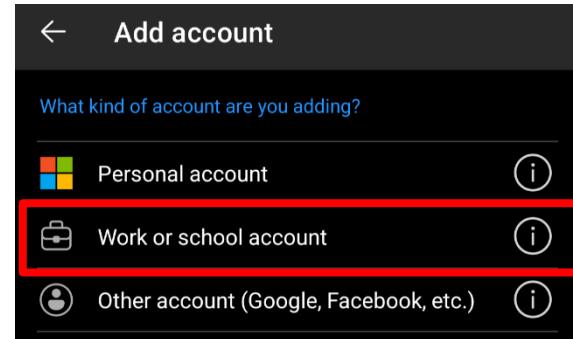
Tap "Scan a QR code".



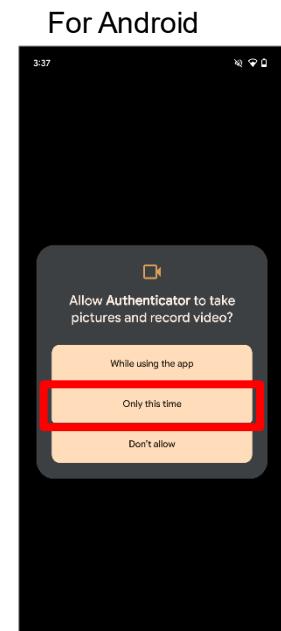
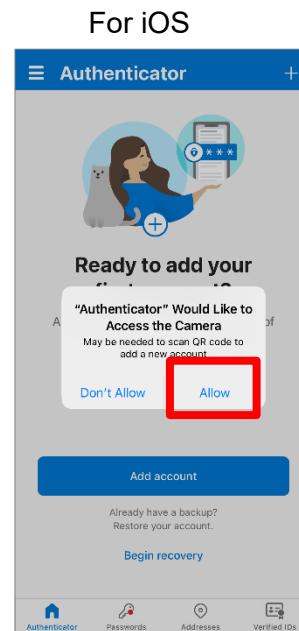
※For Android

1. Tap "Add account".
2. Select "Work or school account".
3. Select "Scan a QR code".

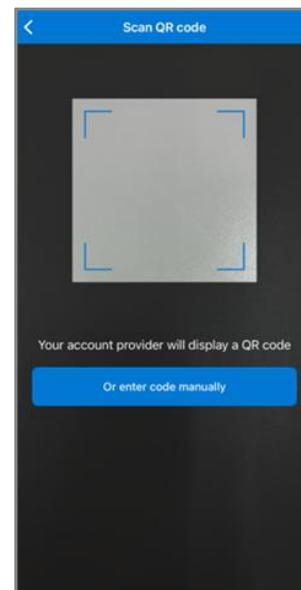




⑤ A message will appear asking for camera access. Select “Allow” or “Only this time”.



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 Authentication 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.**

The top screenshot shows the Microsoft Authenticator app interface. It displays a user profile for "sophia" and a one-time code "927 154" in a red box. The bottom screenshot shows the Sophia University Integrated Authentication System. It features the university's logo and the text "Integrated Authentication System" and "統合認証システム". A warning message in Japanese states: "⚠️ アカウントを有効にするにはモバイル・オーセンティケーターのセットアップが必要です。 (You need to set up Mobile Authenticator to activate your account.)". Below this are two steps: 1. モバイルにアプリ「Microsoft Authenticator」をインストールしてください。 (Please install the app "Microsoft Authenticator" on your mobile.) 2. アプリケーションを開き、バーコードをスキャンします。 (Open the application and scan the barcode.) A QR code is shown for scanning. At the bottom, there is a red box containing a "One-time code" input field, a "Device Name" input field, and a "Submit" button.

4. Other

- If you have changed your smartphone model or uninstalled “Microsoft Authenticator” after setting up multi-factor authentication and need to scan the QR code again, please contact ict-support@sophia.ac.jp for resetting your settings to display the QR code again.
We will reset your settings so that the QR code can be displayed again.
- 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 entered incorrectly even once, or if the screen is left idle for an extended period, the QR code will be refreshed. If the message “Invalid code” continues to appear after multiple attempts, and the cause is not a device change or accidental deletion of a previously registered code, perform the setup again by following the steps in [“3.3. When the Initial Configuration Fails to Load”](#).**

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

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

