Gifu University Integrated Authentication: Multi-factor Authentication User's Manual

Released August 2020

Created by Information & Communications

TABLE OF CONTENTS

1. Overview of Multi-factor Authentication for Integrated Authentication

Gifu University allows for various university systems to be accessed using a single account. This is referred to as "integrated authentication." A user must enter a account only once. A scheme called "single sign-on" (SSO) makes this possible.

Although this is convenient for users, if a set of user ID and password ("account" hereafter) are somehow stolen, it could provide an attacker with external access to Gifu University systems and could result in serious damage both inside and outside the university. In recent years, an increasing number of organizations are implementing multi-factor authentication to prevent this from occurring.

Compared with a conventional authentication in which a user merely enters an account, multi-factor authentication is a scheme that more strongly ensures the authenticity of connections or operations made by the user or registered device that is attempting to be authenticated (i.e., logging into a system or confirming some operation), by making use of a one-time password (*1), biometric authentication (*2), or a dedicated authentication device (*3).

This manual describes what needs to be done in order to use multi-factor authentication (one-time password) for integrated authentication when using the Gifu University system from outside the university, as well as how to use this form of authentication. * When working on university grounds, multi-factor authentication is not required and the user may continue to authenticate as before.

*1 One-time password: A password that is valid only for a certain period of time, or for a certain number of logins

*2 Biometric authentication: A method of authentication that uses information from the body, such as the user's fingerprint or face

*3 Dedicated authentication device: Some examples include inserting a USB dongle into a PC or other system, or scanning an authentication card with a card reader

◆ Who this applies to:

Those who have been issued an individual account from Gifu University to access a Gifu University system

* In cases such as using a email service during a business trip, multi-factor authentication can also be used for the JIMU-account.

◆ Devices that can be registered for use (one device and one email address):
Notebook PCs, tablets, smartphones, etc. purchased using public or personal funds
* Devices should always be carried with the user while on business trips or other excursions.
* The descriptions in this manual mainly assume the use of a smartphone
* Please contact Information Management Core for information on multi-factor authentication for those not affiliated with the university (students of other universities, part-time instructors, etc. who have been issued a Gifu University account) who are generally not on university grounds

◆ Contact information:
Information Management Core 1F
Email: imc-help@gifu-u.ac.jp
Extension: 2041

A1

Flowchart: Multi-factor Authentication for Integrated Authentication

Download the authentication app to the authentication device (your smartphone)

iPhone app, Android app

App not required if using email authentication

(Configure email receipt settings)

Register and configure the authentication device, etc. (required only the first time or when making changes)
(A PC within the university is generally required the first time)

Login to Gifu University Account Manager (GUAM) on the PC and then, on the "SSO User Portal" screen, select either "Account settings" (email) or "One-time password settings" (display QR code)

Use the app to scan the QR code
* Select "Other (Google, Facebook)"
* If you cannot scan, you may instead enter the account name and key code

↓

Enter the one-time password shown in the app using the PC

Configure the email address for sending the one-time password
* It is recommended to register this as a spare, even if primarily using app authentication

Use integrated authentication from outside the university to access university systems (including university email)
*** Required after you begin using multi-factor authentication (not required for use while on university grounds)**

A screen asking you to select the authentication method will appear if you follow the normal procedure and enter an ID and password on the integrated authentication screen

One-time password

↓

Open the app on the registered device, and then enter the one-time password that is displayed

↓

Begin using university systems

One-time password (email authentication)

↓

Enter the one-time password listed in the email sent to the registered email address

↓

Begin using university systems

2. PREPARING FOR USE - STEP 1 (INSTALLING THE APP ONTO THE AUTHENTICATION DEVICE)

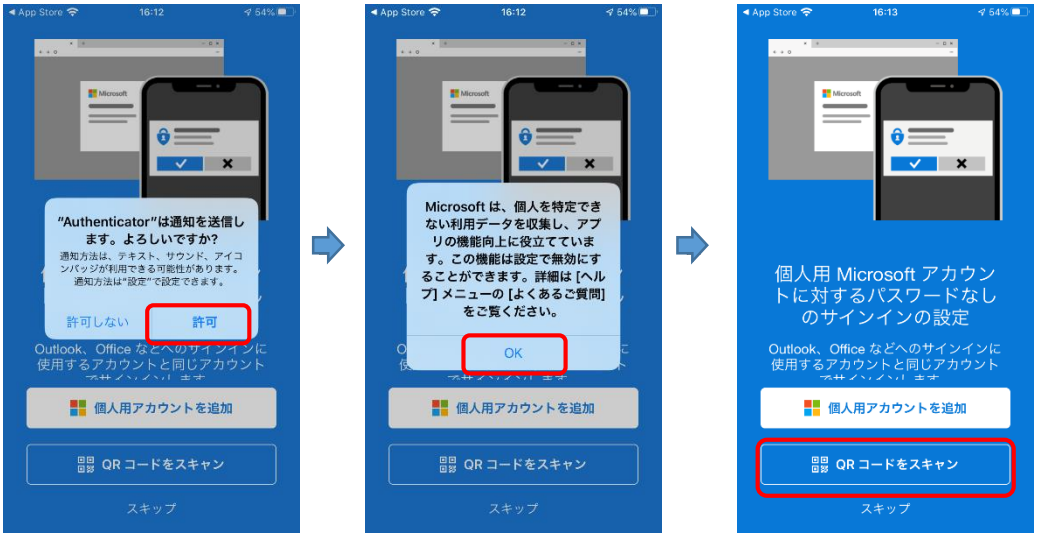
(1) iOS DEVICES (EXPLAINED HERE USING AN iPhone)

① Search for the following app in the App Store and then install it:

"Microsoft Authenticator" (a free app provided by Microsoft).

② You will be asked to confirm the following the first time the app is launched after installing it.

Tap "Allow" for "Send notifications (display notifications on smartphone)" and then tap "OK" for "Privacy (gathering information that cannot be used to identify an individual)."



③ Tap "Scan QR code" to start the QR code camera. If the QR code scanning camera screen appears, proceed to **Preparing for Use - Step 2.**

* If you are asked to provide "access to the camera" during the initial scan, select "OK" and proceed to ④.

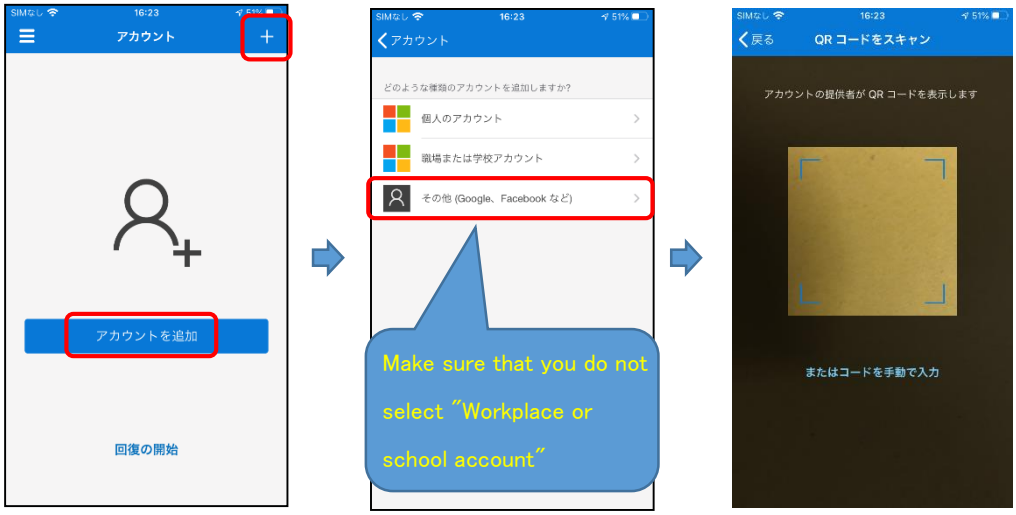
* You may close the app if required.


App Store
16:13
54%
アカウント
"Authenticator"がカメラへのアクセスを求めています
新しいアカウントに追加するには、QR コードをスキャンする必要があるかもしれません
許可しない
OK
アカウントを追加
回復の開始
App Store
16:13
53%
戻る
QR コードをスキャン
アカウントの提供者が QR コードを表示します
または手動でサインイン

④ If you close and then relaunch the app, the order in which the screens are displayed will differ from when the account was configured. Select the screens in the following order to display the QR code camera screen.

＊"Add account" (tap "+" on the upper right to add if already configured) → Other (Google, Facebook, etc.)"

→Camera screen

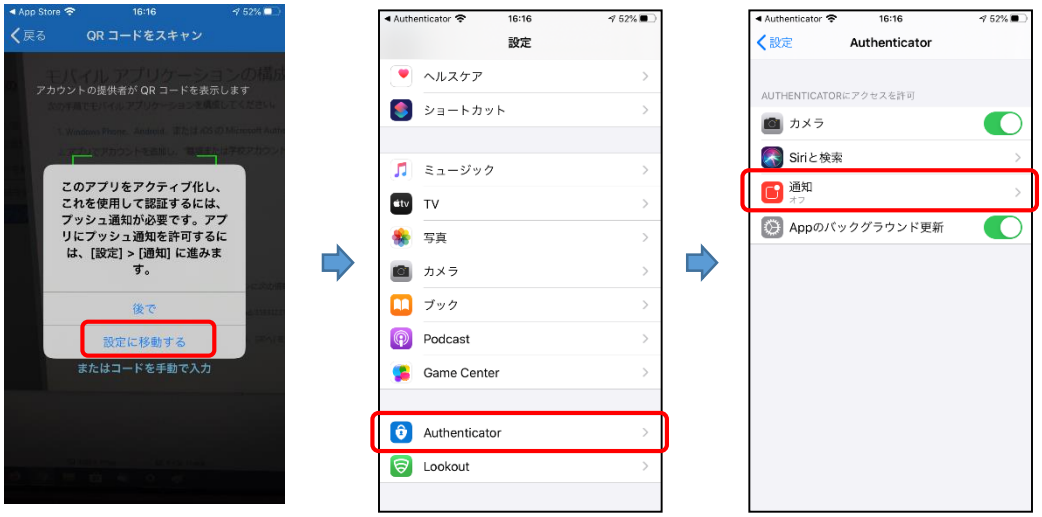


Based on the iOS settings, a function called "App lock" may be enabled when launching an app. This applies even stricter restrictions on app usage, by requiring you to authenticate via fingerprint or facial authentication, or by entering a passcode.

Note that this can be turned OFF in the app settings. However, this is not recommended.

⑤ If a message stating "Activating this app..." appears, follow the procedure below.

1) Go to Settings →Authenticator →Notifications



2) Change "Allow notifications" from OFF (gray) to →ON (green)

* Although several items will be displayed, there is no need to change them.

(2) FOR Android DEVICES (DESCRIBED HERE USING A SMARTPHONE)

① Search for the following app in the Google Play Store and then install it.

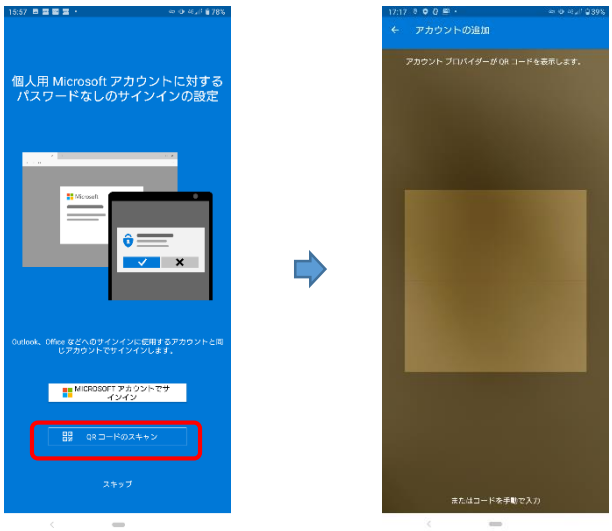
"Microsoft Authenticator" (a free app provided by Microsoft)

② You will be asked to confirm the following the first time the app is launched after installing it.
Tap "Allow" to "Send notifications (display notifications on smartphone)" and then tap "OK" for "Privacy (gathering information that cannot be used to identify an individual)."

③ Tap "Scan QR code" to start the QR code camera. If the QR code scanning camera screen appears, proceed to **Preparing for Use - Step 2.**

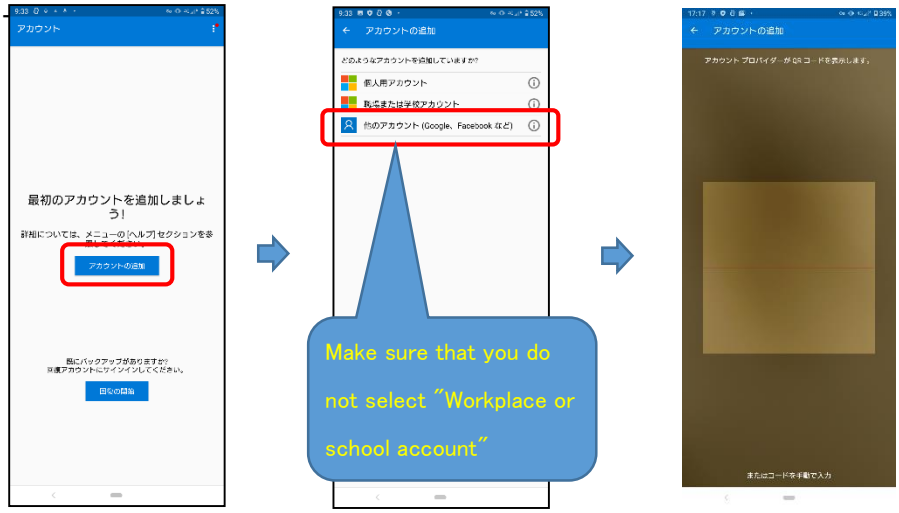
* If you are asked to provide "access to the camera" during the initial scan, select "OK."

* You may close the app if required. However, you will need to follow the procedures described in (1)-④("Add account" → "Other account (Google, Facebook, etc.)" →Camera screen).



④ If you close and then relaunch the app, the order in which the screens are displayed will differ from when the account was configured. Select the screens in the following order to display the QR code camera screen.

＊"Add account" (tap "+" on the upper right to add if already configured) → "Other account (Google, Facebook, etc.)"



(3) To use email authentication

① Configure the email address to use for email authentication so that it can receive email from the "@gifu-u.ac.jp" domain.

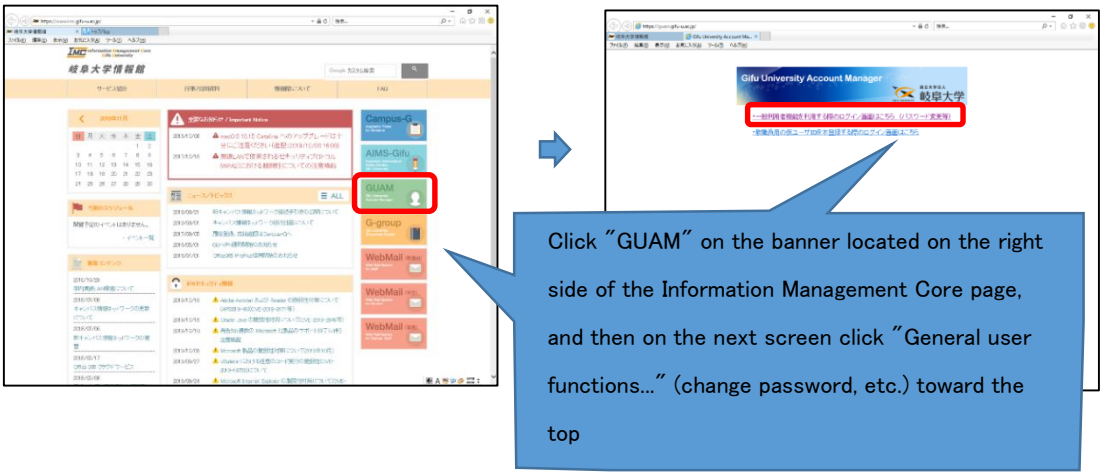
3. PREPARING FOR USE - STEP 2 (ALL DEVICES)

(1) REGISTERING A DEVICE FOR USE IN SYSTEM AUTHENTICATION

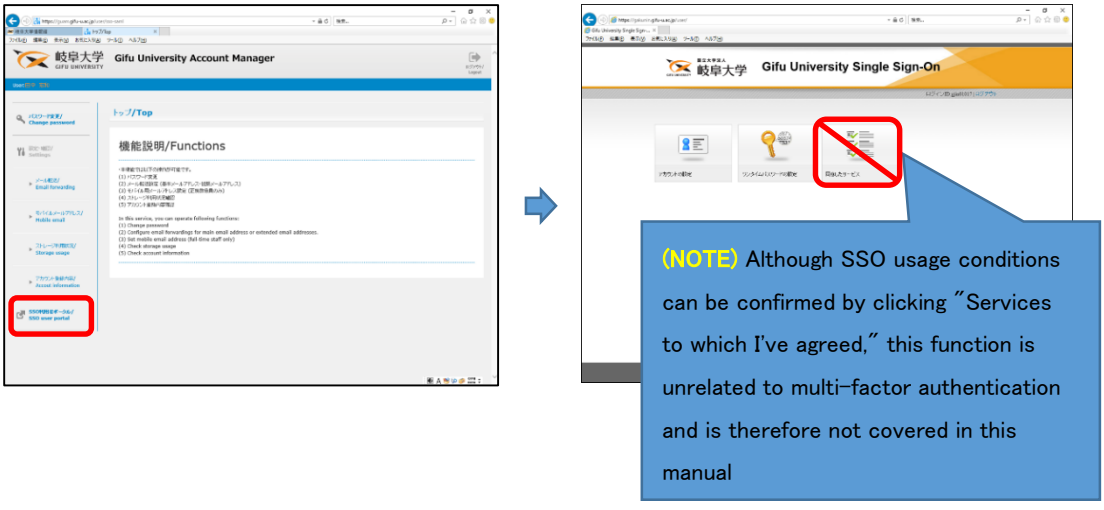
① Open Gifu University Account Manager (GUAM).

* Registering an authentication device is extremely important, so please make sure to do this from a trustworthy PC located on university grounds.

* Please contact Information Management Core for information on multi-factor authentication for those not affiliated with the university (students from other universities, part-time instructors, etc. who have been issued a Gifu University account) who are generally not on university grounds.



② Click "SSO user portal" to display the SSO management screen.



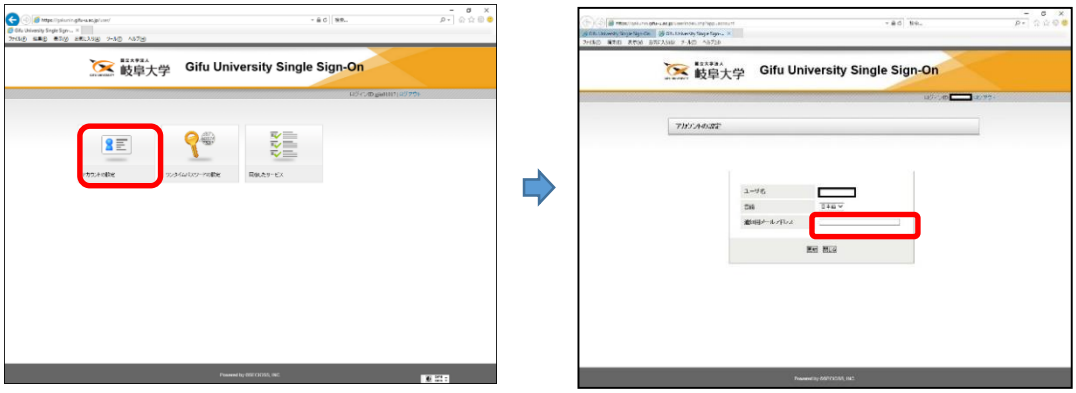
③ To use email authentication (it is recommended to configure this as a backup method)

In "Account settings," set a non-university email addresses for receiving a one-time password. If you set the university email address here, you will be unable

to change it if you fail to authenticate it from outside the university.

* Ensure that the registered email address can receive emails from the "@gifu-u.ac.jp" domain.

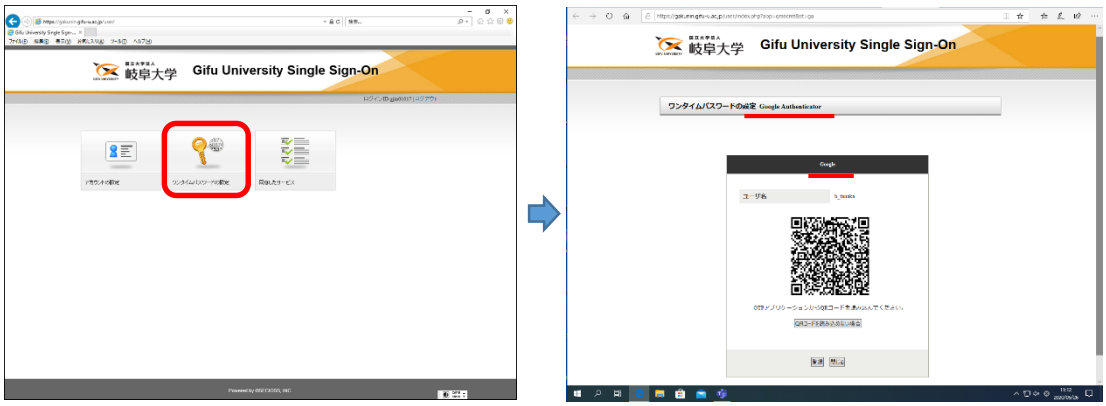
* You can select a language (either Japanese or English), and can set an email address that can be accessed outside of the registered device.



④ To use two-dimensional code authentication

Display a registration QR code from "One-time password settings."

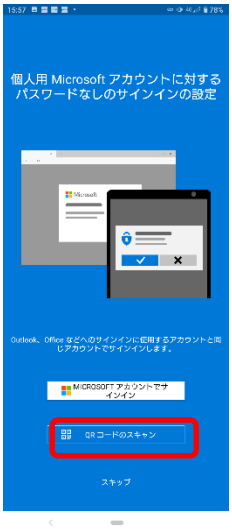
Note that the underlined portions in the figure to the right are "Google Authenticator" and "Google."

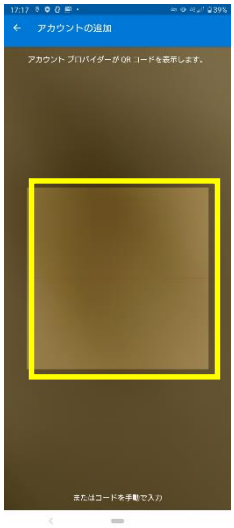


Scan the currently displayed QR code using the Microsoft Authenticator, which you installed earlier on your device.

Launch the app and then prepare to scan the QR code with the camera.

(The procedure is mostly the same for both Android and iOS.)

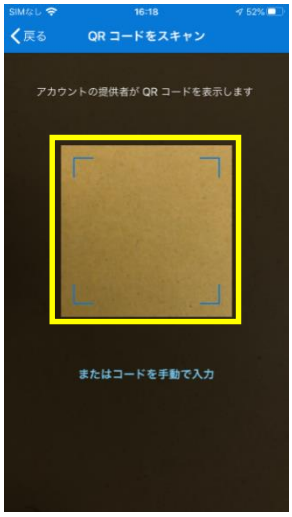




1. Tap "Scan QR code" to display the QR code camera screen.

Select "Other (Google, Facebook, etc.)

* Make sure that you do not select "Workplace or school account"

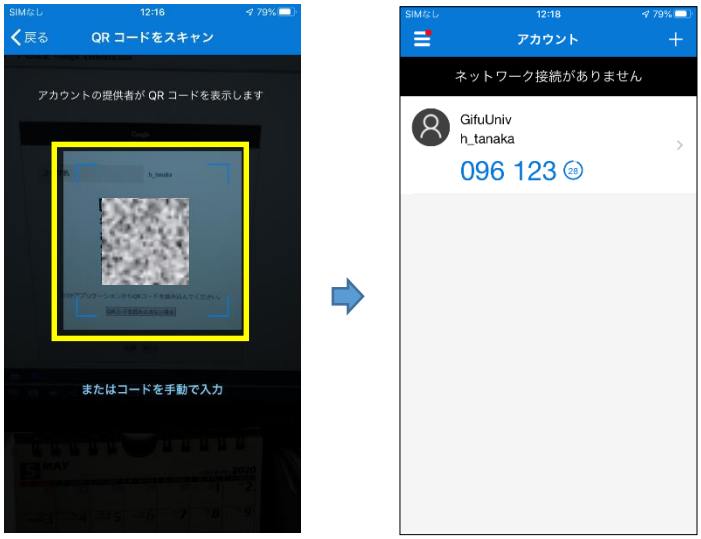


1. Tap "Scan QR code"
2. Tap "Add account"
3. Tap "Other (Google, Facebook, etc.)

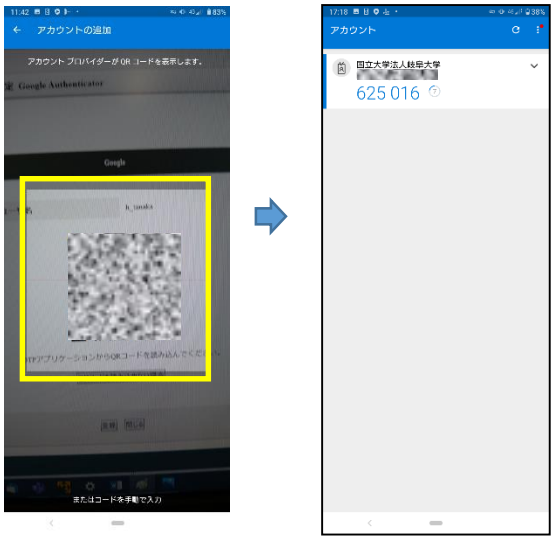
... to display the QR code camera screen

⑤ Adjust the position of your device until the QR code is within the yellow box, and then scan the QR code. If the code is successfully scanned, the app will automatically switch to a screen displaying the one-time password.
Once the one-time password is displayed, proceed to ⑦.

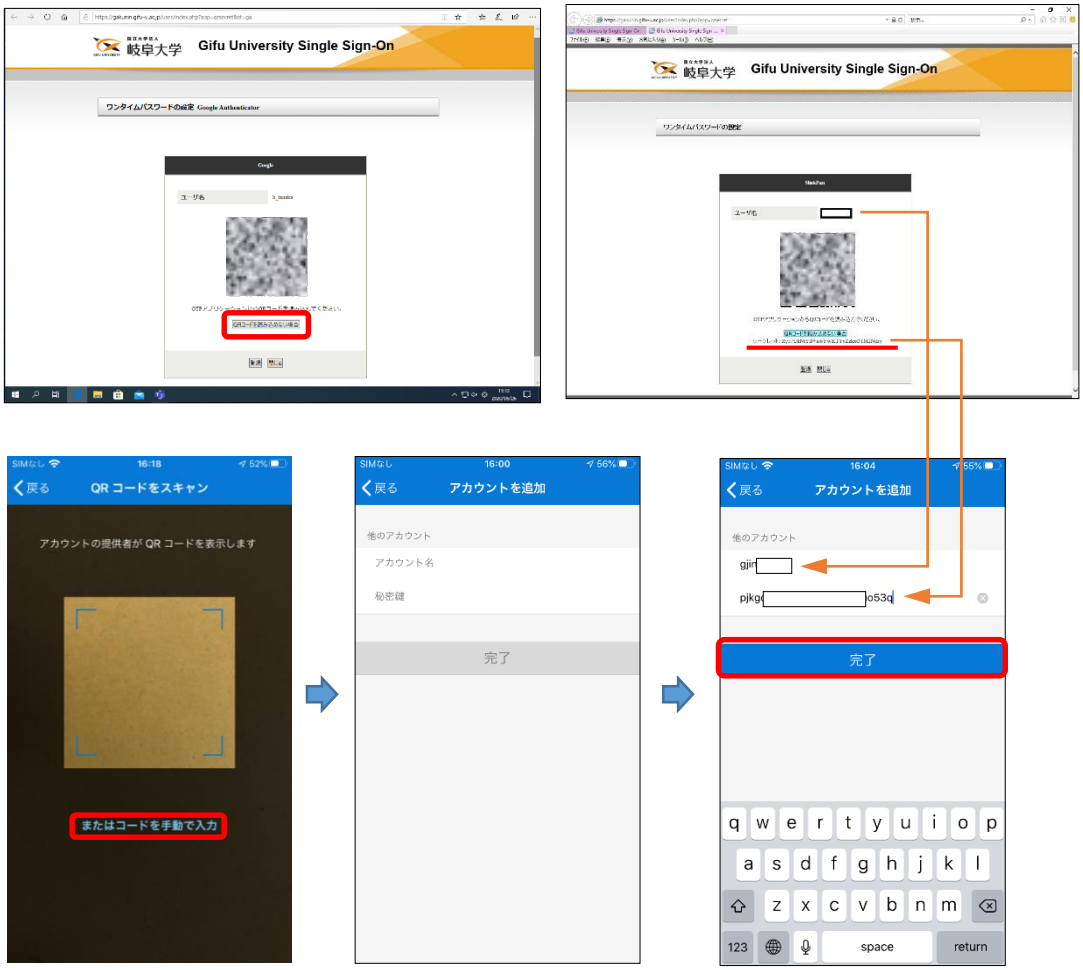
(iOS)



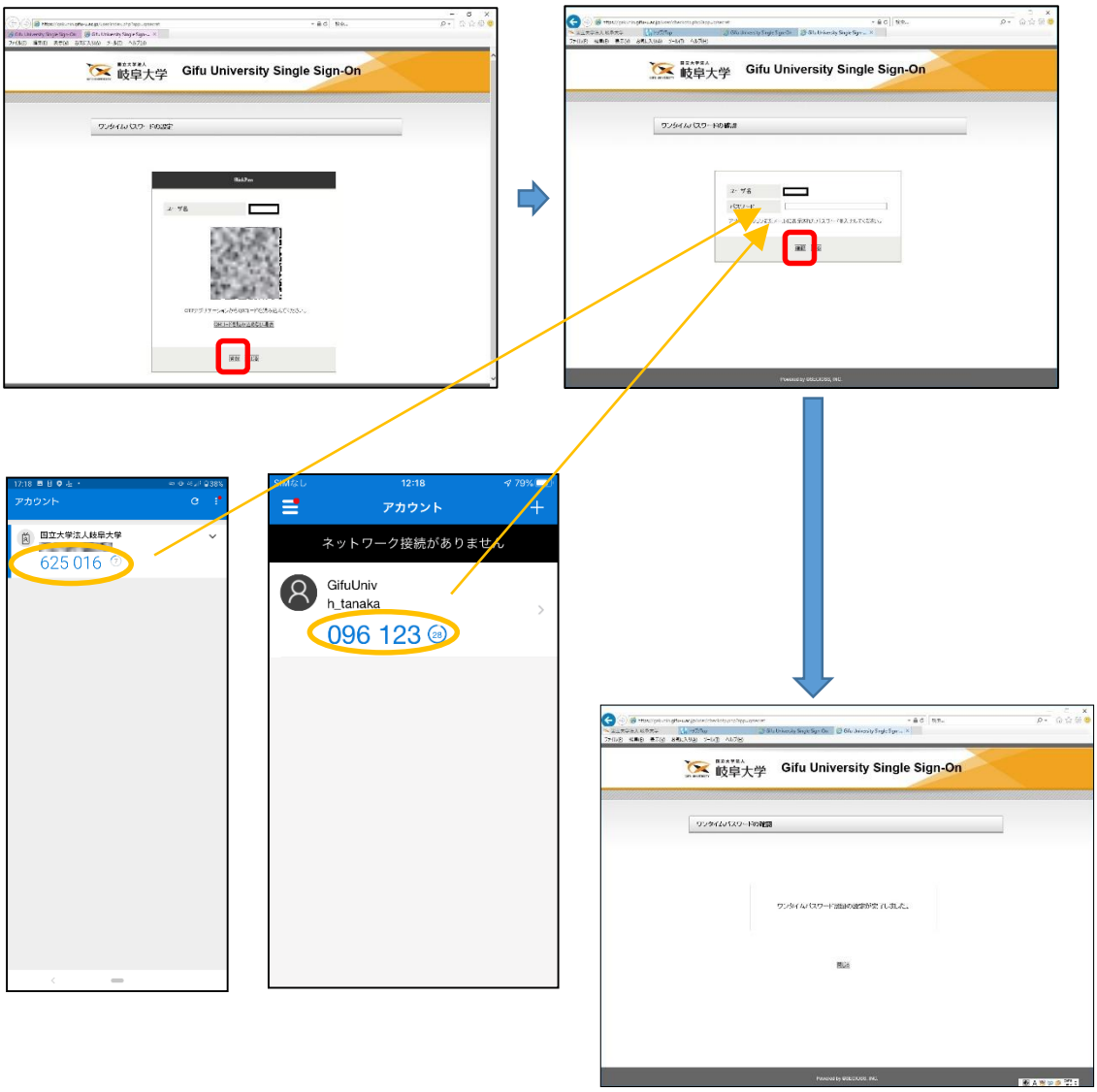
(Android)



⑥ If the QR code cannot be scanned or there are some other issues, you will need to manually register the user and code in the app. On a PC, click the "If the QR code cannot be scanned" button to display the secret code. On the app, tap the "Or manually enter a code" on the bottom of the camera screen. Enter your user name in "Account name" and secret key in "Secret key." Then, tap "Finish."* The text will vary slightly between iOS and Android, proceed to ⑦.



⑦ On the registration screen on the PC, enter the currently displayed one-time password to register the device.



If the device is registered successfully, a message stating that "One-time password authentication has been configured" is displayed.

These settings will not need to be configured on the device from now on, and the one-time password screen will be displayed immediately after launching the "Authenticator" app.

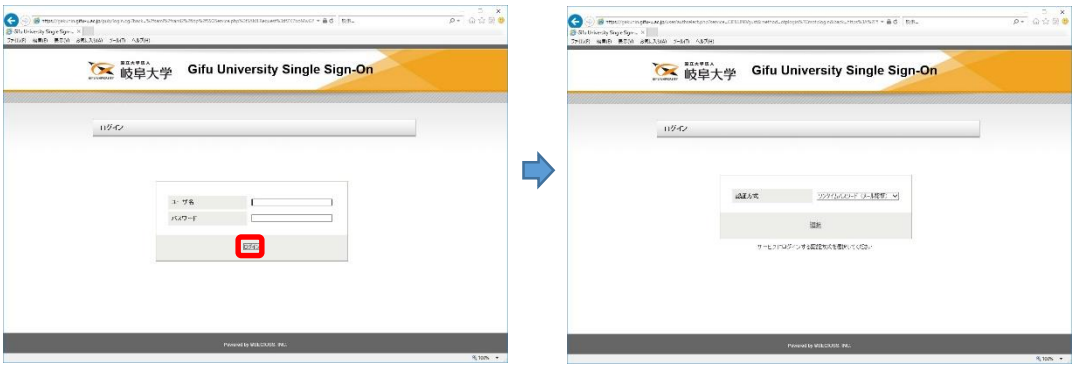
* On Android devices, the one-time password may be displayed on the screen after tapping the account name.

4. HOW TO USE ONE-TIME PASSWORDS

1. Log in to SSO using the same procedure as when on university grounds

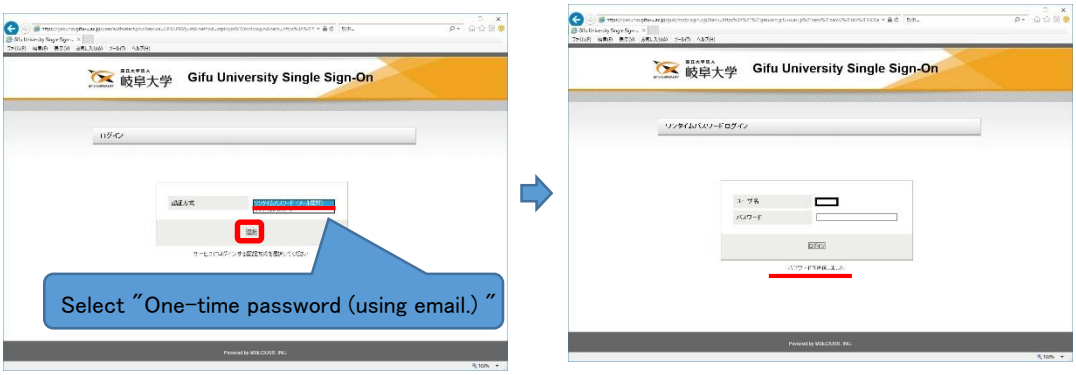
① Log in to the Gifu University system using the same ID and password used as when on university grounds.

When you attempt to log in, you will be asked to select an authentication method. You can select either "One-time password (email authentication)" or "One-time password" as the authentication method. Select an authentication method, and then enter the one-time password using the procedure described below for the selected method. Test site: https://gust.gifu-u.ac.jp Don't save password !

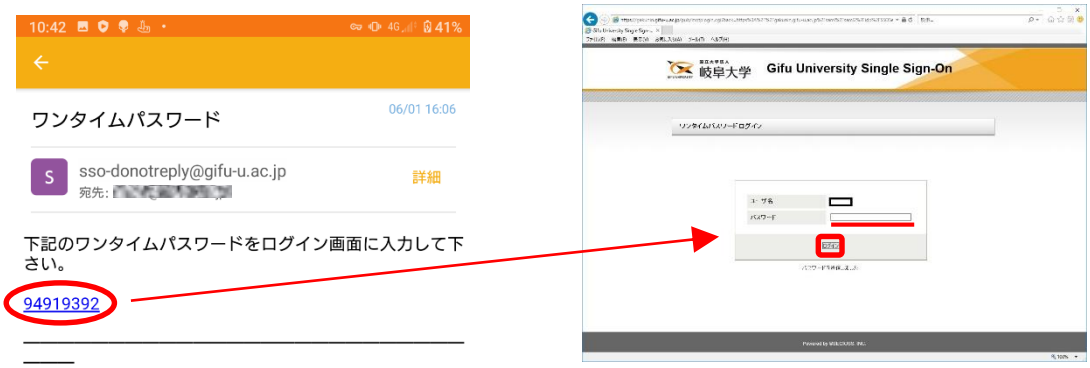


2. Check the one-time password on the registered device (using email)

① The password entry screen is displayed, with "Password sent" displayed on the bottom.



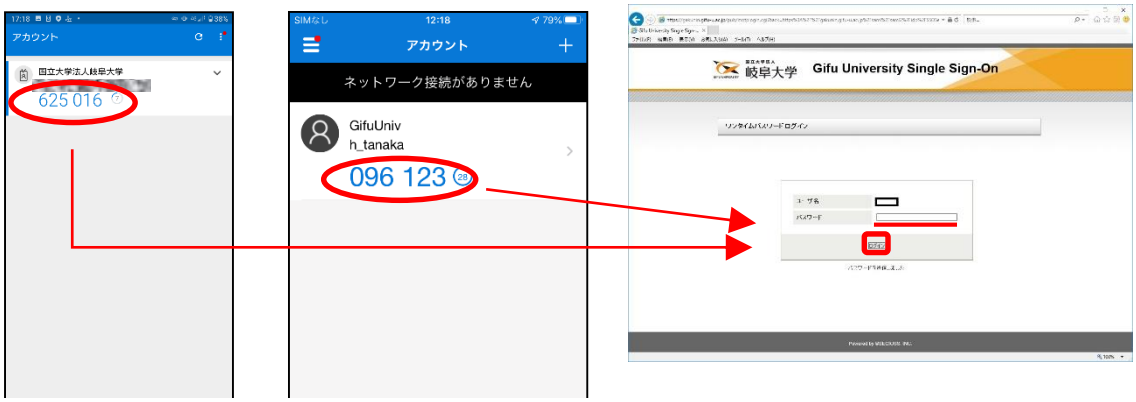
② Open the email (using the registered smartphone or other device), and then enter the currently displayed one-time password on the password entry screen from step 1. Please make sure to delete this email later. Don't save password !



3. Check the one-time password on the registered device (using the app)

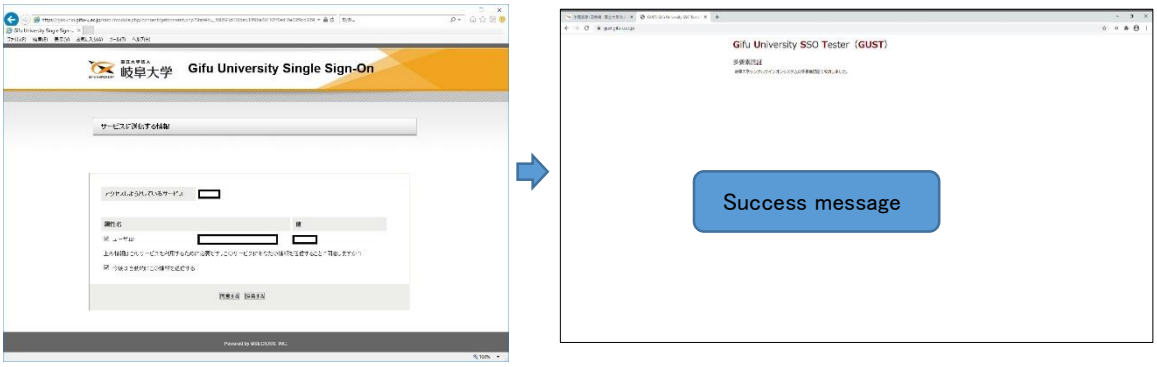
① The password entry screen is displayed.

② Launch the "Authenticator" app (using the registered smartphone or other device), and then enter the currently displayed one-time password on the password entry screen. Please make sure to close the app after using it. Don't save password !



4. Enter the one-time password to log in using SSO

① If the "Information sent to service" screen is displayed to confirm which user information is sent, select "Agree" to log in and begin using the system just as though you were using it on university grounds.



Successfully logging into the test site will display a message stating "Gifu University SSO Tester (GUST)". (You will not be given actual access to a system on the test site.)

5. IMPORTANT NOTES

① Devices and email addresses registered according to the procedures in this manual must be strictly managed in accordance with Gifu University Password Guidelines 3.4 and 3.5. Ensure that these resources are managed and used appropriately.

② Email addresses for receiving one-time passwords registered according to the procedures in this manual must be usable outside of the university and must be set to receive email from the "@gifu-u.ac.jp" domain. It is recommended to confirm an operation assuming use outside the university after registration.

③ Only the most recent registered device and email address are valid among devices/email addresses registered according to this manual. Actions such as leaving the one-time password screen open on a registered device or failing to delete an email after use may unnecessarily allow users other than the intended user to access Gifu University systems. Please make sure to handle information appropriately after use.

④ If you begin using a different device, please make sure to delete any relevant apps, emails, and information from the previous device. You will then need to register the new device.

⑤ If multi-factor authentication is configured for a JIMU-account (or when using email service during a business trip, etc.), please make sure to unregister any email addresses that are no longer needed and delete the app settings after a transfer.
If you take over someone else's JIMU-account, check that his or her settings have been removed.

⑥ The procedure described in "Preparing for Use - Step 2" must generally be done from a PC on university grounds. If you must use a Gifu University system from outside the university but cannot register on university grounds, please contact the Information Management Core through your department.
* No links will be provided in an email on how to prepare for use or begin using this service. Please access this information from the Information Management Core website, or add the link as a favorite on your PC or other device.

⑦ If you lose a registered device, please immediately transfer these settings to another device or email address. If doing so will be difficult, please contact Information Management Core (Email: imc-help@gifu-u.ac.jp　extension 2041).

⑧ If you have any other questions or concerns about use, please contact Information Management Core (Email: imc-help@gifu-u.ac.jp extension 2041).

One-time password test site: https://gust.gifu-u.ac.jp/

* Used in "4. How to Use One-time Passwords" in this manual