Multi-Factor Authentication (MFA)

2021/11/4 version

IMC Account

Easy Setup Guide (1)

What is multi-factor authentication for **IMC accounts**?

- ✓ **An IMC account** is a number, which is a **string of 3 to 8 alphanumeric characters** (for staff) , **lowercasing the first letter of your student number** (for student).
- ✓ An IMC account is used for **Hirodai mail, VPN access and** login for **Office365, Teams**, etc.
- ✓ When accessing from off-campus, authentication by a second factor (a device different from the computer) is required.

Setup instructions page (IMC account)

The setting depends on the device used as the second factor. Please prepare your smartphone, cell phone, or other second devices.

1 Decide the second factor you use

Start → Do you have smartphones or tablets [1]

- Yes → Are voice call or SMS available
  - Yes
    - A. Press the Approve button on the mobile app — procedure 2 → 3A → 4 → 5 **Recommended!**
    - B. Verify the code via short message (SMS) — procedure 2 → 3B → 4 → 5
  - No
    - C. Verify the code on the mobile app — procedure 2 → 3A → 4 → 5
- No → Do you have email address for a cell phone[1]
  - Yes
    - D. Approve by voice operation — procedure 2 → 3C → 4 → 5
  - No → Go to the page (3) “What to do if you don't have a smartphone or cell phone”.

If you are sharing the device with family members etc., Please select “No”.

2 Apply Multi-Factor Authentication using your personal computer

Access the **MFA Configuration for IMC Account** form on your computer browser.

https://mfa.huc.hiroshima-u.ac.jp/mfaweb Access the URL

① Sign-in with your IMC account and password.

② Select "Enable" and send.

③ Confirm that the values is “Enable”
→ Go to Next Step.

3A Setup with mobile app

If you selected "C. Confirm the code with the mobile app and enter it" in step 1, select "Use the confirmation code".

Download the app and read the QR code.

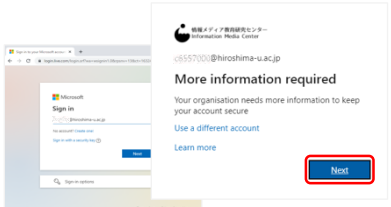
Google Play で手に入れよう　App Store からダウンロード

Download

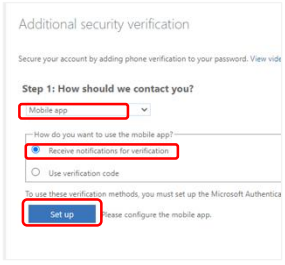
Microsoft Authenticator

① Install [Microsoft Authenticator].

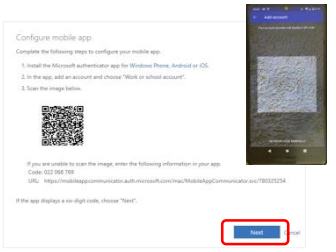
https://mysignins.microsoft.com/security-info



② Sign in Office365 on your computer.
→ Next in [More information required]



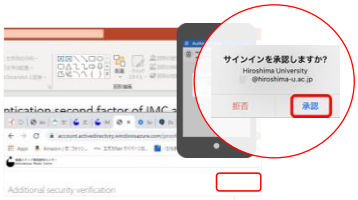
③ Additional security verification
[Mobile App]
→ [Receive notification for verification]
→ [Setup]



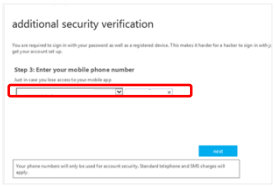
④ Launch the application
→ Add
→ Work or school account
→ Scan the QR code

⑤ After the six-digit number appears on your phone, click [Next].

⑥ Wait until “Mobile apps has been ..” is display, click [Next].



⑦ Tap "Approve" when you receive notification, click [Next].



⑧ Enter your phone number in case you need it, click [Next].

Go to 4

Multi-Factor Authentication (MFA)

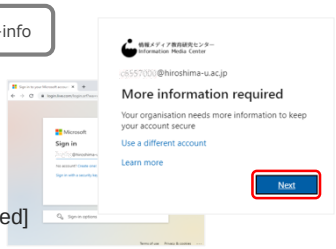
Easy Setup Guide (2)

IMC Account

3B Set up with short massage (SMS)

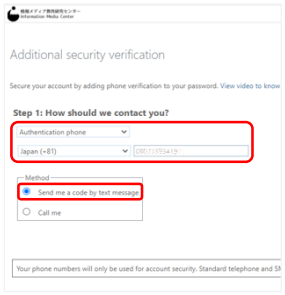
Specify and confirm the phone number to receive the code via SMS.

https://mysignins.microsoft.com/security-info

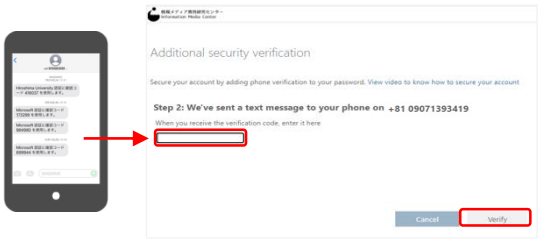


① Sign in Office365 on your computer.
→ Next in [More information required]

② Additional security verification
[Authentication phone]
→ [Country/Region]
→ [Enter your phone number]
→ [Send me a code by text message]
→ [Next]



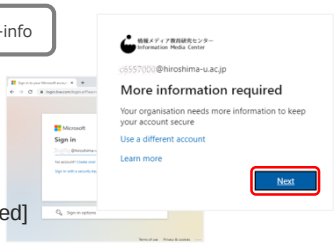
③ When you click [Next], a confirmation code (short message) will be sent to your registered phone number.
→ Input number and [Verify].



3C Set up with voice call

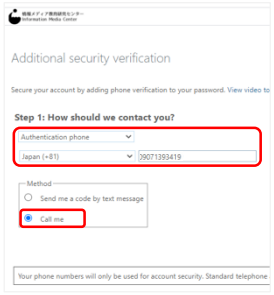
Specify and confirm the phone number to receive voice call.

https://mysignins.microsoft.com/security-info

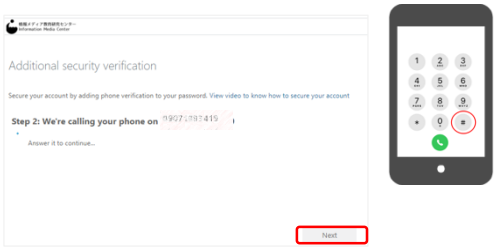


① Sign in Office365 on your computer.
→ Next in [More information required]

② Additional security verification
[Authentication phone]
→ [Country/Region]
→ [Enter your phone number]
→ [Call me]
→ [Next]

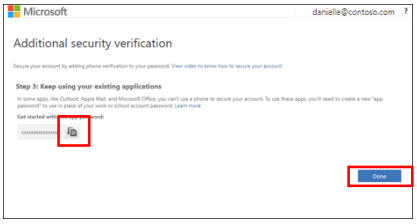


③ When you click [Next], receive voice call and follow the guidance to operate the phone.

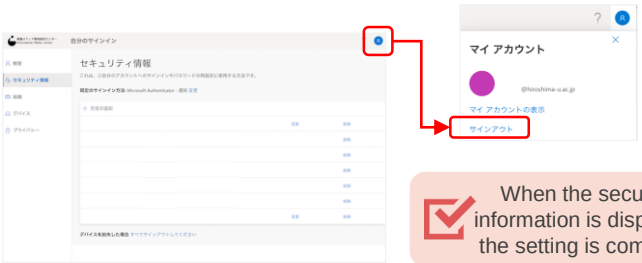


4 Additional security settings (application password)

Finally, after confirming the app password, sign-in to the portal to complete the settings.
The application password is a password (16 random characters) issued to use applications (such as email client) that do not support MFA.
You can get the app password later.



① “Step3: Keep using your existing applications” will be displayed.
Please make a note of app password and click “Done".



When the security information is displayed, the setting is complete .

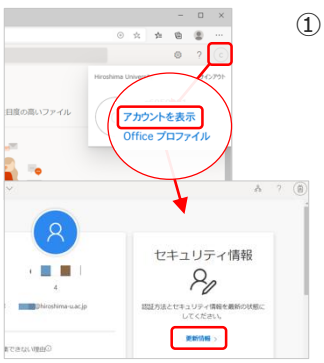
② [Security Information] page will appear,
click [Sign Out] from the profile icon.

How to get the app password or change the second factor after setting multi-factor authentication

If you want to change the settings after setting up MFA, you can do this from the Office365 portal.

① Sign-in to Office365
Click on the profile icon in the upper right corner .
→ View your account
→ Security Information > [Update Information].

In the case of getting the application password.
[Add Method → App Password]
In the case of changing the second factor.
[Change the "sign-in method”]



Multi-Factor Authentication (MFA)

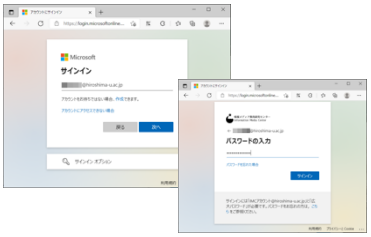
Easy Setup Guide (3)

IMC Account

5 Confirm the MFA configuration after set up

Finally, let's confirm whether multi-factor authentication actually works.
Multi-factor authentication will be skipped when you access from the campus network, so please use an off-campus network (such as home or tethering from smartphone, eduroam, etc.) to check the operation.

https://portal.office.com



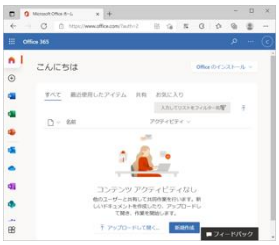
① Access Office365 on your computer

[Approve on the mobile app]

[Verify the code by SMS]

[Approve by voice operation]

② Authenticate with the second factor



③ Login completed

Please be sure if you use an email client

Hirodai Mail (Microsoft365 Exchange Online) supports advanced/modern authentication (OAuth2.0).

If you want to use your email client after setting up MFA, you will need to set either the advanced/modern authentication or the app password. You cannot send or receive e-mails without changing the settings.

Advanced/modern authentication is an authentication method that uses a mechanism called an access token to ensure higher security in order to solve the security problems of conventional authentication using IDs and passwords (basic authentication).It is possible to access email service with multi-factor authentication by using mail client that supports advanced/modern authentication.

Microsoft's release states that basic authentication will be discontinued after October 2022. Take advantage of this opportunity to use an email client that supports advanced authentication or the latest Microsoft or Apple email client.

Email clients that support advanced authentication (as of October 2021)
Outlook app for iOS/Android, macOS/iOS standard email client,
Thunderbird (78.3.1 or later), Becky! Internet Mail (v2.75.02 or later), etc.

How to configure Thunderbird for Oauth2.0 is introduced on the IMC website.

IMC Webpage
→ All Services
→ Hirodai Mail
→mail software
→ Example configuration for Thunderbird

https://bit.ly/2XFSL8h

When in trouble

- Is there any way to check the current configuration status?
  - ✓ When sign in an Office365 from an off-campus network (home, smartphone tethering, eduroam, etc.), if you are asked for the second factor, multi-factor authentication is enabled.
- After setting up MFA, I can no longer send or receive Hirodai email. What should I do?
  - ✓ If you are using e-mail software that does not support multi-factor authentication, you will need to set an app password. Please check "Additional security settings (application password)" on the previous page.
- What should I do if I want to disable multifactor authentication due to trouble?
  - ✓ From the campus network (HU-CUP, etc.), disable the setting according to Step.2.

IMC FAQ Site

⚠What to do if you don't have a smartphone or a cell phone

Multi-factor authentication can be performed using an extension of the web browser of the computer being used.
Please use this service only if you set a login password on your computer and manage it well so that it cannot be used by others.

FAQ page
https://help.media.hiroshima-u.ac.jp/index.php?solution_id=1170

For inquiries about the setting method, please contact
Information Media Center
https://www.media.hiroshima-u.ac.jp

Multi-Factor Authentication (MFA)

2022/7/1 version

HIRODAI ID

Easy Setup Guide (1)

What is multi-factor authentication for **HIRODAI ID**?

- ✓ **A Hirodai ID** is a staff number, student number, or user registration card number (e.g., **B209999**)
- ✓ Login to **My Momiji, Iroha, Bb9**, etc.
- ✓ When accessing from off-campus, authentication by a second factor (a device different from the computer) is required.

Instruction webpage (HIRODAI ID)

The setting depends on the device used as the second factor. Please prepare your smartphone, cell phone, or other second devices.

1 Decide the second factor you use

Start → Do you have smartphones or tablets [1]

- yes → A. Verify the code on the mobile app. Procedure 2→ 3A→ 4 **Recommended!**
- No → Do you have email address for a cell phone [1]
  - yes → B. Verify the code via email. Procedure 2→ 3B→ 4
  - No → C. Verify the code with the backup code. Procedure 2→ 3C→ 4

If you are sharing the device with family members etc., Please select “No”.

Go to the page (2) “What to do if you don't have a smartphone or cell phone”.

2 Apply Multi-Factor Authentication using your personal computer

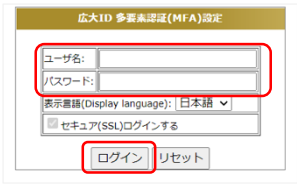
Access the **IMC Registration System** with your computer browser.

Access the following URL

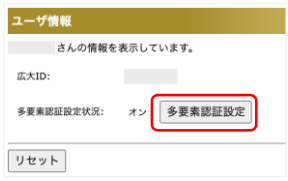
https://reg.huc.hiroshima-u.ac.jp

① Enter your password from [Login by HIRODAI ID]

② Click [広大ID] in menu ☰ → Multi-Factor Authentication Settings



③ Login with HIRODAI ID and password



④ Click [Multi-Factor authentication Settings]

Next, proceed to the settings for either 3A, 3B, or 3C.

3A Set up with the mobile app

Download the app and read the QR code.

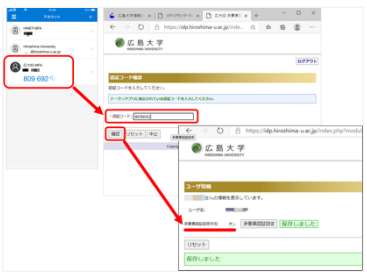
Google Play で手に入れよう / App Store からダウンロード

Download

Microsoft Authenticator

① Install [Microsoft Authenticator].

② Launch the application → Add → Work or school account → Scan the QR code.

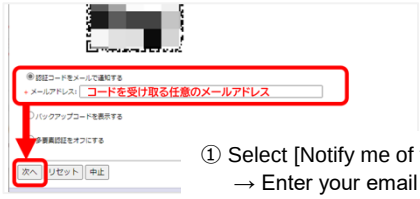


③ The code displayed on the application (6 digits) in the Authentication Code field to confirm.

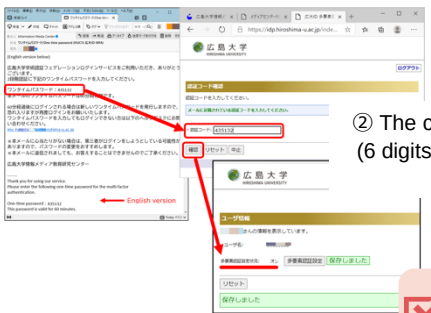
When the MFA status is [**ON**], the setting is complete .

3B Set up with the email address

Specify the email address (except for a HIRODAI Mail) to receive the code.



① Select [Notify me of the authentication code by e-mail]. → Enter your email address to receive the code.



② The code displayed on the application (6 digits) in the Authentication Code field to confirm.

When the MFA status is [**ON**], the setting is complete .

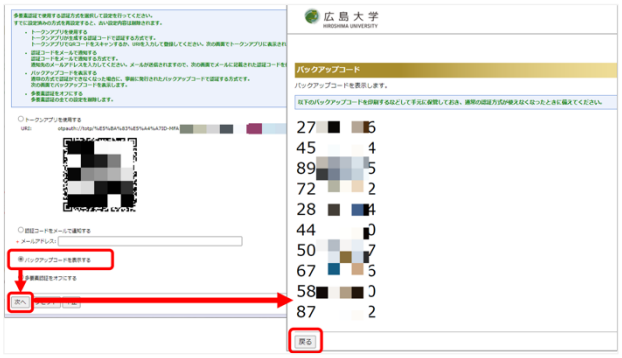
Multi-Factor Authentication (MFA)

Easy Setup Guide (2)

HIRODAI ID

3C Get the backup code

The backup code is to allow you to log in even if you cannot authenticate your phone app or authenticate via email.



When the MFA status is [**ON**], the setting is complete .

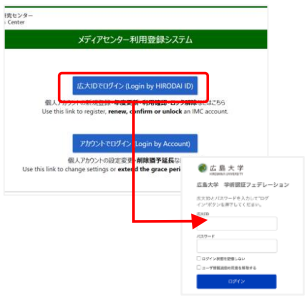
Select [Show backup code].
→ Record the 10 codes that are displayed.

4 Confirm the MFA configuration after set up

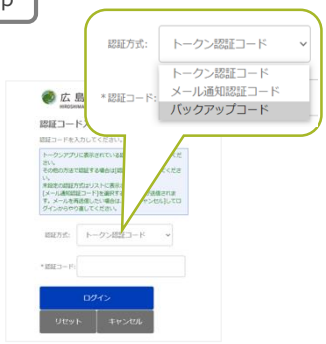
Finally, let's confirm whether multi-factor authentication actually works.
Multi-factor authentication will be skipped when you access from the campus network, so please use an off-campus network (such as home or tethering from smartphone, eduroam, etc.) to check the operation.

https://reg.huc.hiroshima-u.ac.jp

① Access the IMC Registration System

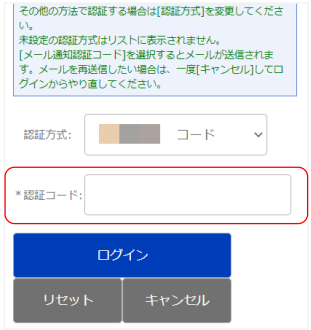


② Login with HIRODAI ID and password.



③Select [Authentication method].

④ Authenticate with the second factor



⑤ Enter the code to **complete the login.**

When in trouble

- Is there any way to check the current multi-factor authentication status?
  - ✓ If you are prompted to enter a code after entering your password when logging in to IROHA or MOMIJI from an off-campus network (such as home or smartphone tethering), the setting is enabled.
- What should I do if I change my phone?
  - ✓ You will need to change the authentication method. You will need to change the authentication method. If you are on the campus network (HU-CUP, etc.), the second factor will be skipped, so please connect to the campus network and change the authentication method.
- How do I disable multifactor authentication setting?
  - ✓ Select [Turn off multi-factor authentication] according to "Section 2. Enable Multi-Factor Authentication using your personal computer".

IMC FAQ Site

⚠ What to do if you don't have a smartphone or a cell phone

Multi-factor authentication can be performed using an extension of the web browser of the computer being used.
Please use this service only if you set a login password on your computer and manage it well so that it cannot be used by others.

FAQ page
https://help.media.hiroshima-u.ac.jp/index.php?solution_id=1170

For inquiries about the setting method, please contact
Information Media Center
https://www.media.hiroshima-u.ac.jp