Easy Setup Guide (1)

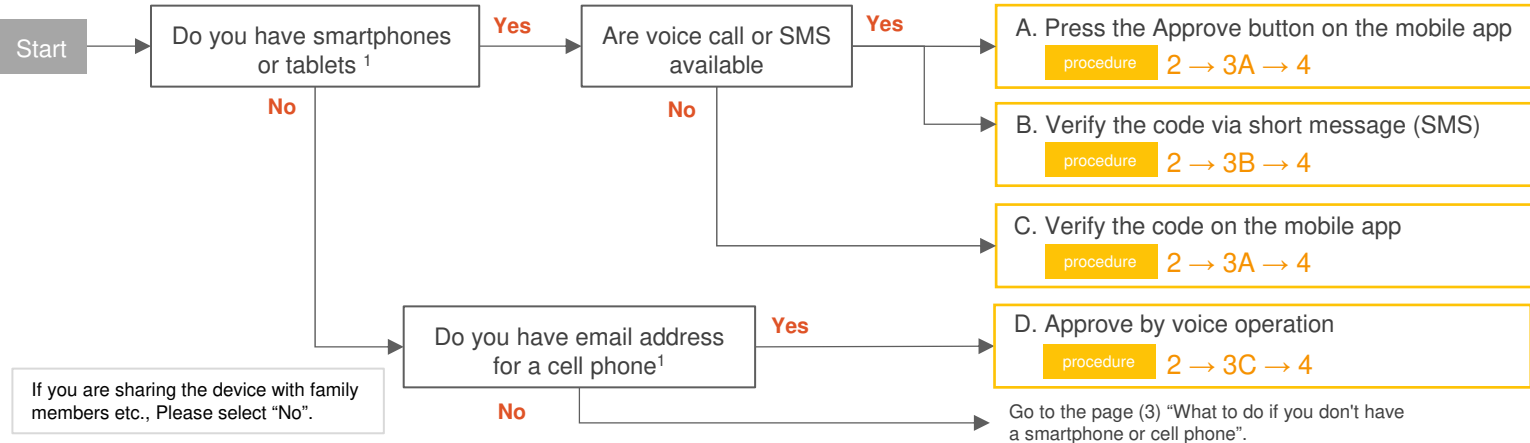👍 What is multi-factor authentication for **IMC accounts**?

- ✓ **An IMC account** is a number, which is a **string of 3 to 20 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 **Microsoft365, 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

No ↓ (Are voice call or SMS available)

B. Verify the code via short message (SMS)
procedure 2 → 3B → 4

C. Verify the code on the mobile app
procedure 2 → 3A → 4

Do you have smartphones or tablets [1] — **No** → Do you have email address for a cell phone[1] — **Yes** →

D. Approve by voice operation
procedure 2 → 3C → 4

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

Do you have email address for a cell phone[1] — **No** →

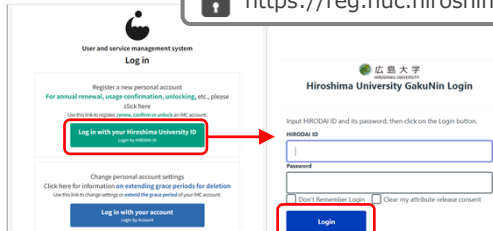Go to the page (3) "What to do if you don't have a smartphone or cell phone".

2 Setup using your personal computer

Access the **User and service management System** with your computer browser and apply to [login by HIRODAI ID].

① Access the URL https://reg.huc.hiroshima-u.ac.jp

※ If you are "setting up for the first time" ,you can configure it directly from steps [3A], [3B], and [3C] instead of through the "Service Management System."
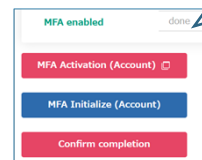
If MFA is already set up for your account, the "MFA Initialize(Account)" button will be displayed. If you have MFA set up for your account but cannot authenticate, please click "MFA Initialize(Account)" first, then click "MFA Activation (Account)".

② Enter your Hirodai ID and password from [Login by HIRODAI ID] and Click [login]

IF you log in from an off-campus network and the message " MFA has not been setup yet." is displayed, please configure MFA for your HIRODAI ID first.
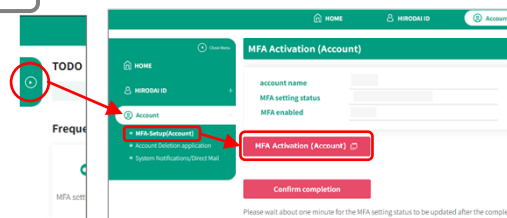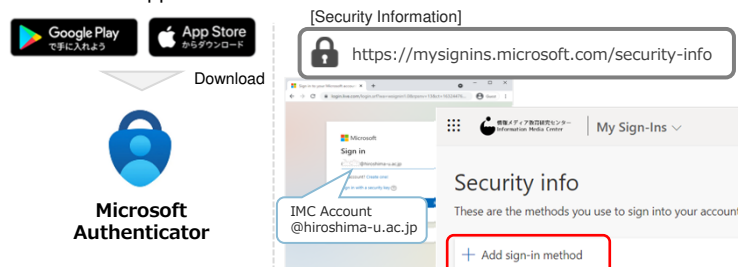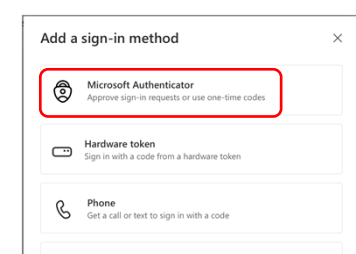
③ Click the triangle arrow in the upper left corner
→ Click [Account] → Click [MFA-Setup(Account)]
→ Click [MFA Activation(Account)]

3A Setup with mobile app

Download the app and read the QR code.

Google Play / App Store — Download

Microsoft Authenticator

[Security Information]
https://mysignins.microsoft.com/security-info
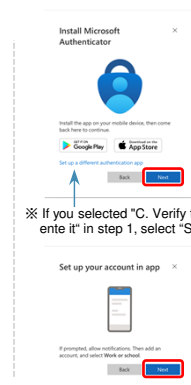
IMC Account @hiroshima-u.ac.jp

① Install [Microsoft Authenticator].

② Sign in Microsoft365 [Security info] on your computer. → [Add sign-in method]
※ If the [Keep your account secure] screen is displayed, click [Next] and go to ④

Add a sign-in method:
- Microsoft Authenticator — Approve sign-in requests or use one-time codes
- Hardware token — Sign in with a code from a hardware token
- Phone — Get a call or text to sign in with a code

③ Click [Microsoft Authenticator] app

④ Click [Next]
※ If you selected "C. Verify the code on the mobile app and ente it" in step 1, select "Set up a different authenticator app".
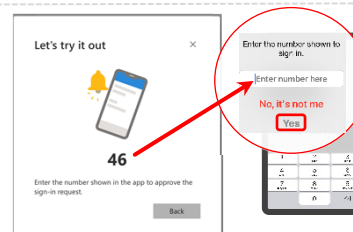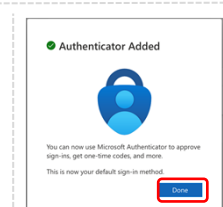
⑤ Click [Next]

< Phone screen > <PC screen>
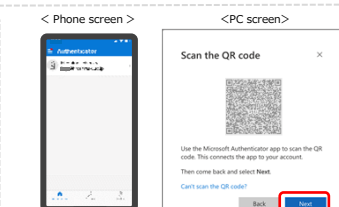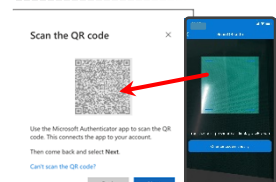
⑥ Launch the application
→ + [Add]
→ [Work or school account]
→ [Scan the QR code]

⑦ " Hiroshima University IMC account@hiroshima-u.ac.jp" appears on your phone, click [Next].

⑧ Enter the notified number into the smartphone app, Tap [Yes].

⑨ Click [Done].
Go to 3B or 4

Please enter your phone number in case you need it.

3B Set up with short massage (SMS)

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

[Security Information] 🔒 https://mysignins.microsoft.com/security-info

① Sign in Microsoft365
  [Security info] on your computer.
  → [Add sign-in method]

※ If the [Keep your account secure] screen
  is displayed, click [Next] and go to
  [Set up another method] in the lower-left.

IMC Account
@hiroshima-uac.jp

Security info
These are the methods you use to sign
+ Add sign-in method
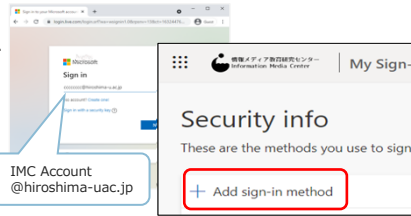
② Click [Phone]

③ [Select a country code]
  [Enter your phone number]
  → [Text a code] → [Next]

④ A confirmation code (short message)
  will be sent to your registered
  phone number.
  → Input number and [Next].

⑤ " Phone number added "
  is displayed, Click [Done]

Verify your phone number
Enter the code we sent to +81
475274
Didn't receive the code?
Next

Phone number added
You can now receive a code each time you sign in.
Done

3C Set up with voice call

Specify and confirm the phone number to receive voice call.

[Security Information] 🔒 https://mysignins.microsoft.com/security-info
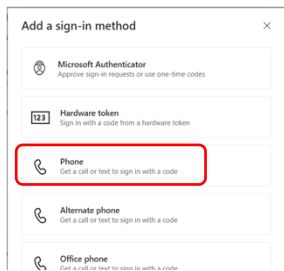
① Sign in Microsoft365
  [Security info] on your computer.
  → [Add sign-in method]
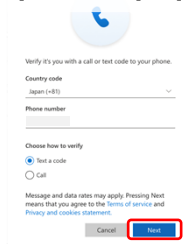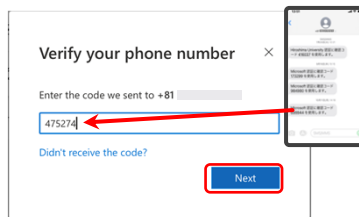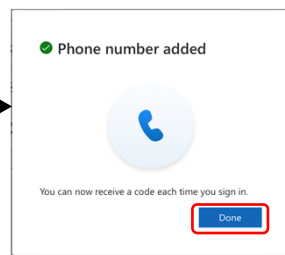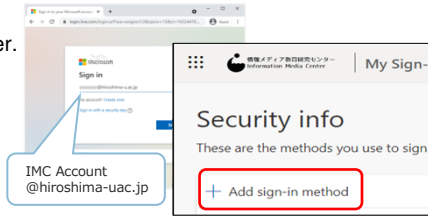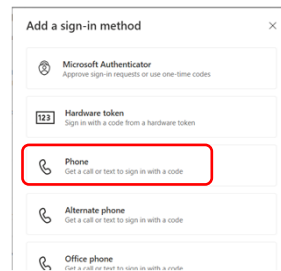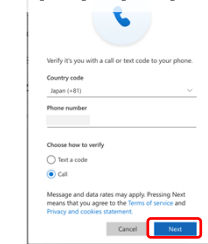
※ If the [Keep your account secure] screen
  is displayed, click [Next] and go to
  [Set up another method] in the lower-left.

IMC Account
@hiroshima-uac.jp

Security info
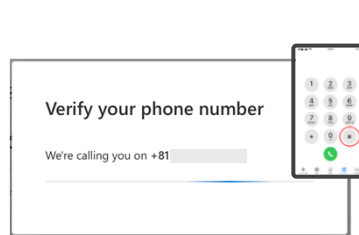These are the methods you use to sign
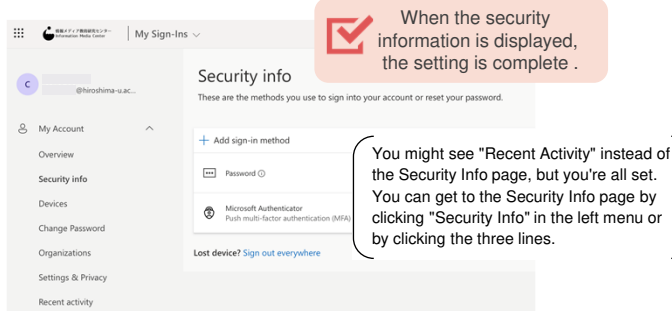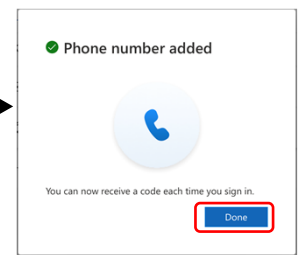+ Add sign-in method

② Click [Phone]

③ [Select a country code]
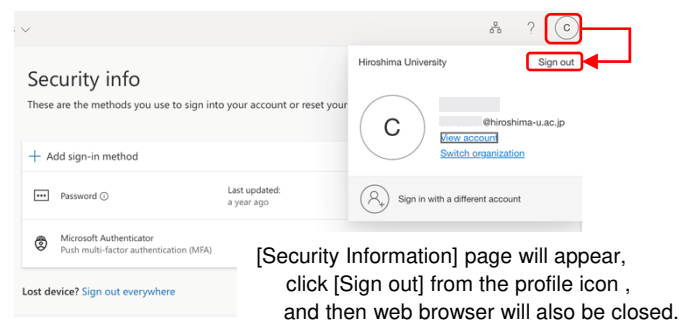 [Enter your phone number]
  → [Call] → [Next]

④ Receive voice call and follow
  the guidance to operate the phone.

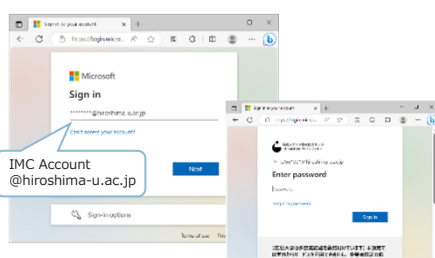⑤ " Phone number added "
  is displayed, Click [Done]

Verify your phone number
We're calling you on +81

Phone number added
You can now receive a code each time you sign in.
Done

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

Security info
These are the methods you use to sign into your account or reset your password.
+ Add sign-in method
Password ⓘ
Microsoft Authenticator
Push multi-factor authentication (MFA)
Lost device? Sign out everywhere

You might see "Recent Activity" instead of
the Security Info page, but you're all set.
You can get to the Security Info page by
clicking "Security Info" in the left menu or
by clicking the three lines.

Security info
These are the methods you use to sign into your account or reset your
+ Add sign-in method
Password ⓘ   Last updated: a year ago
Microsoft Authenticator
Push multi-factor authentication (MFA)
Lost device? Sign out everywhere

Hiroshima University
@hiroshima-u.ac.jp
View account
Switch organization
Sign in with a different account
Sign out

[Security Information] page will appear,
  click [Sign out] from the profile icon ,
  and then web browser will also be closed.

Go to 4

4 Confirm the MFA configuration after set up

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

IMC Account
@hiroshima-u.ac.jp

[Approve on the mobile app]

Approve sign in request
Open your Authenticator app, and enter the
number shown to sign in.
No numbers in your
to the latest version.
I can't use my Microsoft
**

[Verify the code by SMS]

Verify your identity
Text +XX XXXXXXXXXX
Call +XX XXXXXXXXXX
More information
Are your verification methods correct? Check at
https://aka.ms/mfasetup

Enter code
We texted your phone +XX XXXXXXXXXX.
Please enter the code to sign in.
Code
More information
click
Verify

Approve sign in request
We're calling your phone. Please answer it to
continue.
Having trouble? Sign in another way
More information
click

[Approve by voice operation]

Security Info
Security info
These are the methods you use to sign into your account or reset your password.
You're using the most advisable sign-in method where it applies.
Sign-in method when most advisable is unavailable. Authenticator app or hardware token - code Change
+ Add sign-in method
Phone   +81   Change Delete
Password ⓘ   Last updated: 7 months ago Change
Microsoft Authenticator iPhone 12 Delete
Push multi-factor authentication (MFA)
Authenticator app Delete
Time-based one-time passcode (TOTP)
Lost device? Sign out everywhere

② Access Office365 [Security Information]
  on your computer

④ Authenticate with the second factor

⑤ Login completed

## 🔍 How to add 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 Microsoft365 site [Security Information] .

① Sign in Microsoft365 [Security info] on your computer.

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

When you access [Security Information] from the campus network,
you will be asked for multi-factor authentication. Please authenticate
before accessing the site.

② ・In the case of adding a second factor.
[Click the "Add sign-in method"]
・In the case of changing the phone number.
[Click the "Change"]
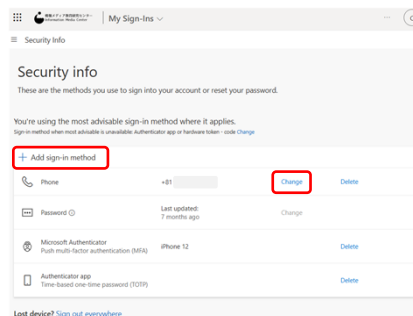
◆ If the second factor authentication is not available, please refer to "How to reconfigure the application (multi-factor authentication for IMC accounts)".
(https://www.media.hiroshima-u.ac.jp/services/mfa/mfa4imcaccount/mfa-imc-app-resetting/)
Click to access the page

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 the advanced/modern
authentication. 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.

Thank you for your understanding and 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 have changed my phone or a deleted the authentication application?
  - ✓ You need to reconfigure. Please follow the instructions of "How to add or change the second factor after
    setting multi-factor authentication" or "How to reconfigure the application(multi-factor authentication for
    IMC accounts" to reconfigure second factor.
- What should I do if I want to disable multifactor authentication due to trouble?
  - ✓ You cannot disable, but you can initialize. In setting according to Step 2, select "Multi-factor
    authentication initialize (Account)" and reconfigure.

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