

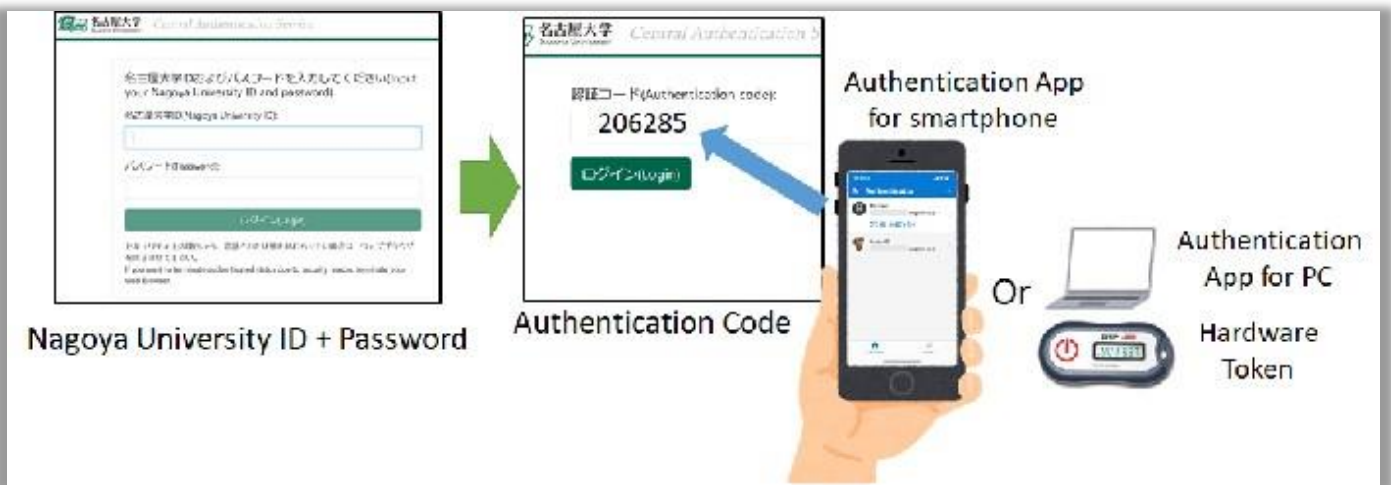
How to setup Multi-Factor CAS authentication account

1.1st Edition

26/1/2022

Multi-Factor Authentication CAS

In addition to the Nagoya University ID and password, authentication for Multi-Factor Authentication CAS requires an "Authentication Code" which is a 6-digit number that changes at 30 second intervals (see below figure).



The Authentication Code is presented on an Authentication Application - which has an Authentication Seed registered - or a hardware token. The hardware token requires additional expenses to purchase, so we recommend you to use the Authentication Application as far as possible.

Registering a new Authentication Seed to an Authentication Application

The following are registration procedures for common Authentication Applications.

- [Authentication Seed Registration to Google Authenticator](#)
- [Authentication Seed Registration to Microsoft Authenticator](#)
- [Authentication Seed Registration to WinAuth \(Windows App\)](#)
- [Authentication Seed Registration to Step Two \(macOS App\)](#)

Contents

Authentication Seed Registration to GoogleAuthenticator 3

Authentication Seed Registration to Microsoft Authenticator..... 9

Authentication Seed Registration to WinAuth (Windows App) 14

Authentication Seed Registration to Step Two (macOS App) 23

Trial Run of Multi-Factor Authentication CAS..... 29

Application to Use Hardware Token for Multi- Factor Authentication CAS 32

Authentication Seed Registration to Google Authenticator

Google Authenticator Setup

Install Google Authenticator onto your smartphone from [Google Play \(Android\)](#) or the [App Store \(Apple\)](#).



Login to the Authentication Seed Management webpage and Authentication Seed generation

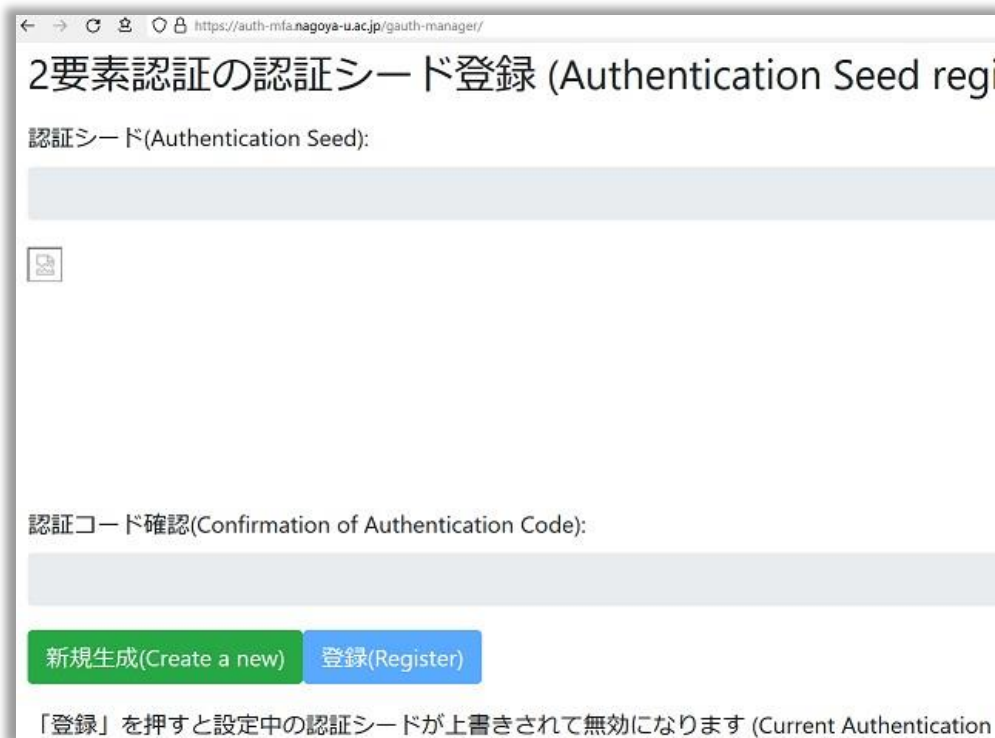
When you connect to the [Multi-Factor Authentication CAS Authentication Seed Management webpage](#), the system requires authentication with your Nagoya University ID and password, so please input them to authenticate.

To distribute Authentication Seeds safely, access to the Authentication Seed Management webpage is only allowed from the Nagoya University's network on campus excluding special case.

A screenshot of the Nagoya University Central Authentication Service login page. The browser address bar shows the URL: https://auth-mfa.nagoya-u.ac.jp/cas/login?service=https%3A%2F%2Fauth-mfa.nagoya-u.ac.jp%2Fgauth-manager%2F&renew=false. The page header includes the Nagoya University logo and the text '名古屋大学 NAGOYA UNIVERSITY' and 'Central Authentication Service'. The main content area has a heading '名古屋大学IDおよびパスワードを入力してください(Input your Nagoya University ID and password)'. Below this are two input fields: '名古屋大学ID(Nagoya University ID):' and 'パスワード(Password):'. A green 'ログイン(Login)' button is below the fields. At the bottom, there is a security notice in Japanese and English: 'セキュリティ上の理由から、認証された状態を終わらせたい場合は、ウェブブラウザを終了させて下さい。 If you want to terminate authenticated status due to security reason, terminate your Web Browser.' On the right side, there is a green box titled 'GAuth Manager' with an icon of a globe and server, and text: '2要素認証のための認証シード (Seed for Two Factor Authentication)'.

If you click the "Create a new" button, a new Authentication Seed will be generated.

You cannot display a previously used Authentication Seed. Similar to other password reset procedures, you can only generate and register a new Authentication Seed.



2要素認証の認証シード登録 (Authentication Seed registration)

認証シード(Authentication Seed):

認証コード確認(Confirmation of Authentication Code):

新規生成(Create a new) 登録(Register)

「登録」を押すと設定中の認証シードが上書きされて無効になります (Current Authentication Seed will be overwritten and become invalid when 'Register' is pressed)

The generated Authentication Seed will be displayed as both an "Authentication Seed" (consisting of alphanumeric characters) and a "QR code".



2要素認証の認証シード登録 (Authentication Seed registration)

認証シード(Authentication Seed):

H88M5G942C23L

認証コード確認(Confirmation of Authentication Code):

090795

新規生成(Create a new) 登録(Register)

「登録」を押すと設定中の認証シードが上書きされて無効になります (Current Authentication Seed will be overwritten and become invalid when 'Register' is pressed)

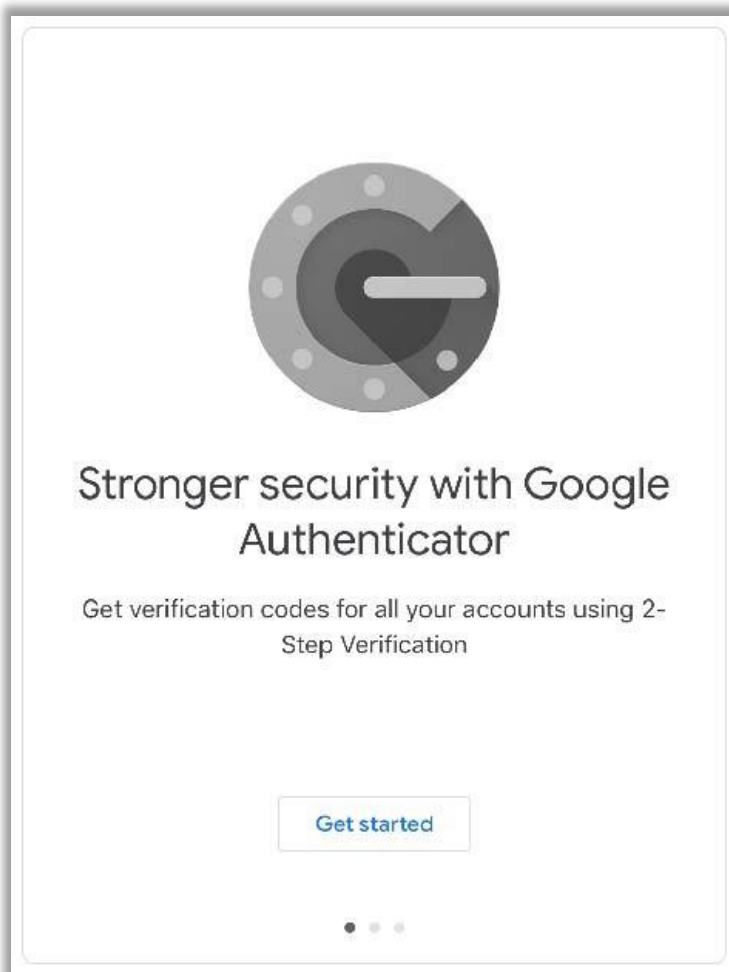
The Authentication Seed will not be registered to the CAS server until you click the "Register" button on the Authentication Seed Management webpage. **After you register the Authentication Seed to the Authentication Application, please remember to click the "Register" button** to register the Authentication Seed to the CAS server.

Even if you mistakenly generate a new Authentication Seed, the previous Authentication Seed will remain as long as you do not click the "Register" button. Be sure to close the Multi-Factor Authentication CAS Authentication Seed Management webpage without clicking the "Register" button.

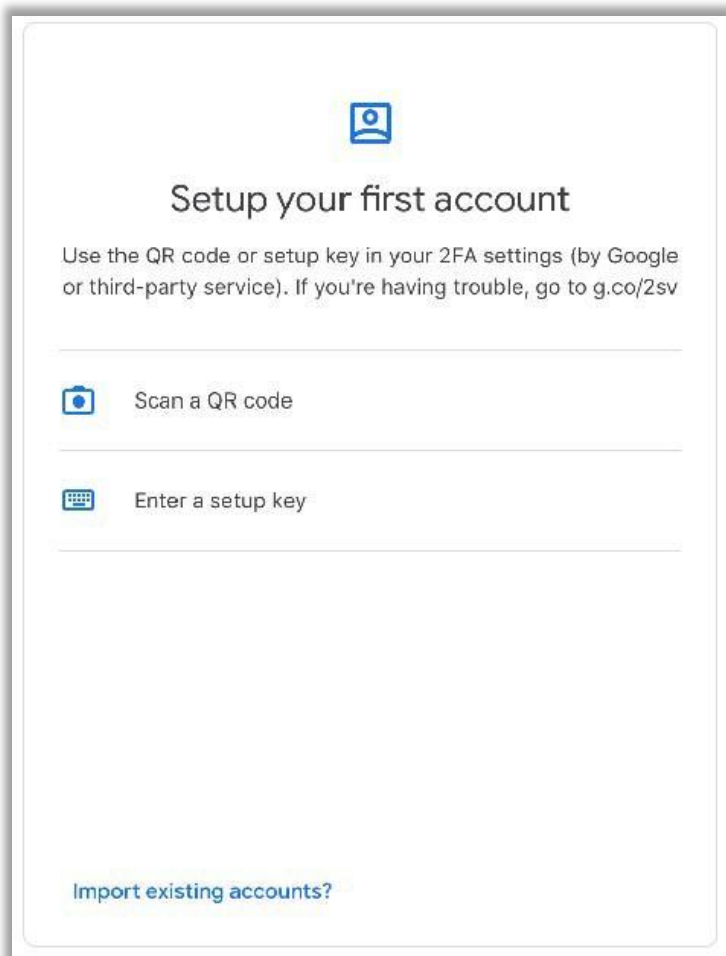
Procedure to register an Authentication Seed to Google Authenticator

For first-time users of Google Authenticator

When you start Google Authenticator, you will see the following screen. Tap "Get started" to proceed.



Next, a screen to select a method to register your Authentication Seed will appear. Select "Scan a QR code". You will receive a notification on your smartphone, "Authenticator requires permission to use your camera". Allow it.



For people already using Google Authenticator

After starting Google Authenticator, tap the "+" mark on the lower right-hand corner of the screen and start the registration of a new Authentication Seed.

Next, a screen to select a method to register your Authentication Seed will appear. Select "Scan a QR code".



Authentication Seed registration with a QR code

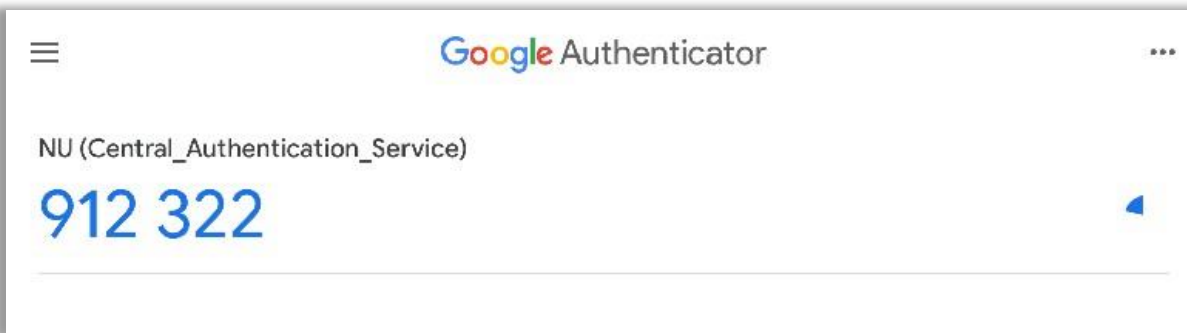
If you choose "Scan a QR code" with a smartphone that has a built-in camera, a QR code scan screen will appear. Scan the QR code displayed on the Authentication Seed Management webpage.

The Authentication Seed will be registered as "NU (Central_Authentication_Service)".

Confirm that the 6-digit number displayed in the "Confirmation of Authentication Code" field on the Authentication Seed Management webpage is the same as the one shown on Google Authenticator.

If they are not the same, the time on your smartphone may be greatly out of sync.

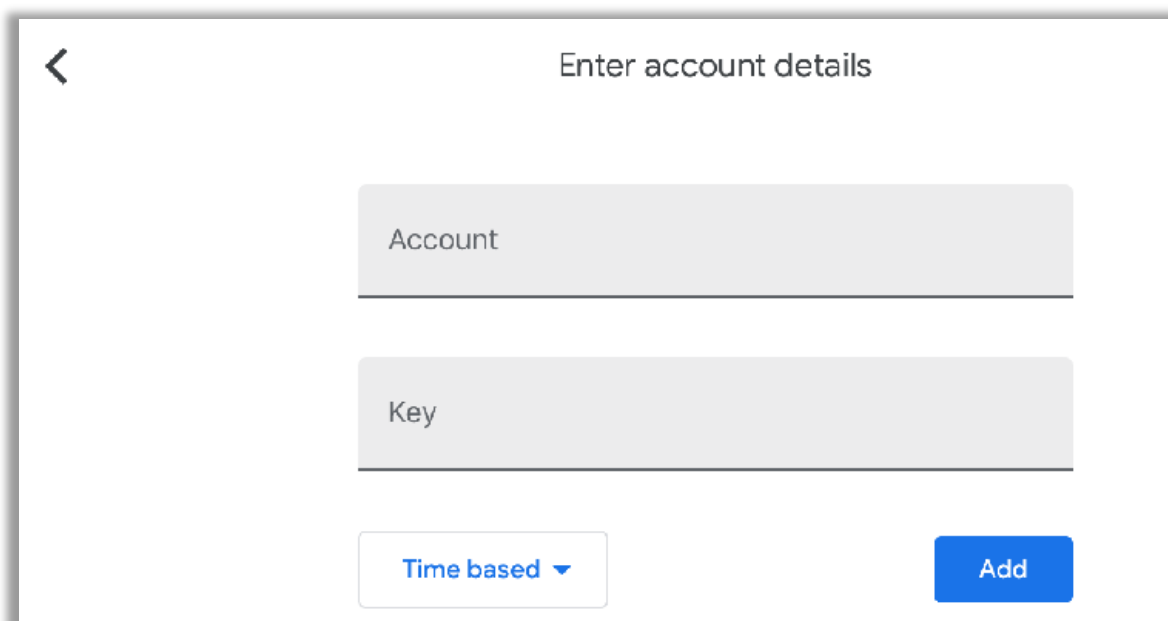
After confirming that the 6-digit number displayed in the "Confirmation of Authentication Code" field is the same as the one shown on Google Authenticator, **please remember to click the "Register" button on the Multi-Factor Authentication CAS Authentication Seed Management webpage** and register your Authentication Seed to the CAS server.



Authentication Seed registration by manually inputting the Authentication Seed (Setup Key)

If you select "Enter a setup key" when registering a new Authentication Seed, the following Setup Key (Authentication Seed) registration screen will be shown.

- Set an "Account name" that you can remember.
- Do not use an account name that is easily identifiable as being connected to your Nagoya University ID. Select "Time based" for "Key Type".
- Input your "Authentication Seed" in the "Key" field.
- The authentication is not case sensitive, so you may input alphabetic characters in lower case letters if you wish.
- It may be difficult to distinguish between characters like "0" (zero) and "O" and "1" (one) and "I", but feel free to input them as you like since those characters are handled as the same.



Confirm that the 6-digit number displayed in the "Confirmation of Authentication Code" field on the screen is the same as the one shown on Google Authenticator.

If they are not the same, the time on your device may be greatly out of sync.

After confirming that the 6-digit number displayed in the "Confirmation of Authentication Code" field is the same as the one shown on Google Authenticator, **please remember to click the "Register" button on the Multi-Factor Authentication CAS Authentication Seed Management webpage** and register your Authentication Seed to the CAS server.

Trial Run of Multi-Factor Authentication CAS

We have prepared a [Multi-Factor Authentication CAS Trial webpage](#) to carry out a trial run of the Multi-Factor Authentication CAS. Following the instructions on the [Trial Run of Multi-Factor Authentication CAS webpage](#).

Authentication Seed Registration to Microsoft Authenticator

Microsoft Authenticator Setup

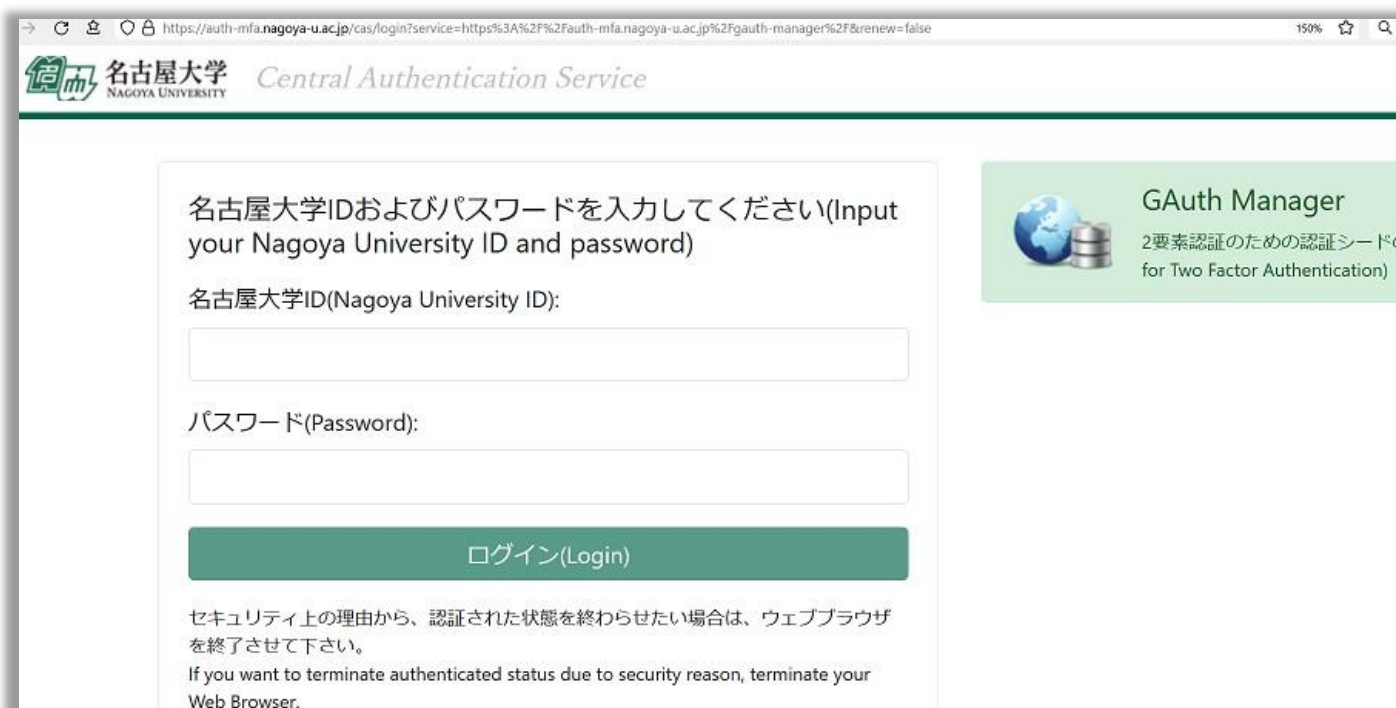
Install Microsoft Authenticator onto your smartphone from [Google Play \(Android\)](#) or the [App Store \(Apple\)](#).



Login to the Authentication Seed Management webpage and Authentication Seed generation

When you connect to the [Multi-Factor Authentication CAS Authentication Seed Management webpage](#), the system requires authentication with your Nagoya University ID and password, so please input them to authenticate.

To distribute Authentication Seeds safely, access to the Authentication Seed Management webpage is only allowed from the Nagoya University's network on campus excluding special case.



名古屋大学 NAGOYA UNIVERSITY Central Authentication Service

名古屋大学IDおよびパスワードを入力してください(Input your Nagoya University ID and password)

名古屋大学ID(Nagoya University ID):

パスワード(Password):

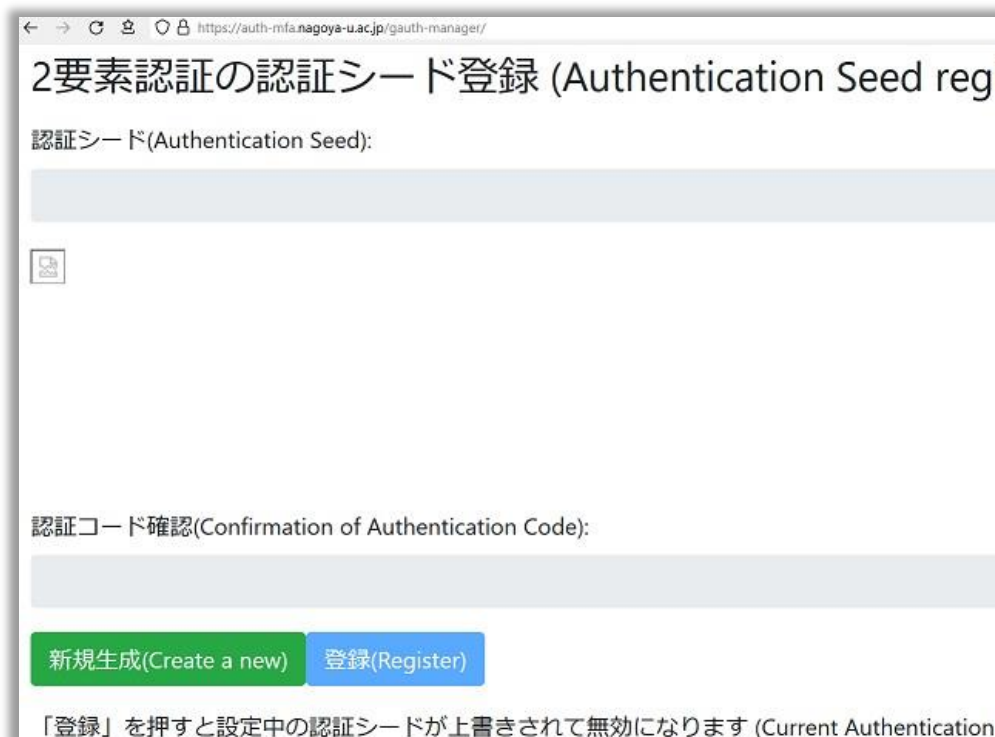
ログイン(Login)

セキュリティ上の理由から、認証された状態を終わらせたい場合は、ウェブブラウザを終了させて下さい。
If you want to terminate authenticated status due to security reason, terminate your Web Browser.

GAuth Manager
2要素認証のための認証シード
(Seed for Two Factor Authentication)

If you click the "Create a new" button, a new Authentication Seed will be generated.

You cannot display a previously used Authentication Seed. Similar to other password reset procedures, you can only generate and register a new Authentication Seed.



2要素認証の認証シード登録 (Authentication Seed registration)

認証シード(Authentication Seed):

認証コード確認(Confirmation of Authentication Code):

新規生成(Create a new) 登録(Register)

「登録」を押すと設定中の認証シードが上書きされて無効になります (Current Authentication Seed will be overwritten and become invalid when 'Register' is pressed)

The generated Authentication Seed will be displayed as both an "Authentication Seed" (consisting of alphanumeric characters) and a "QR code".



2要素認証の認証シード登録 (Authentication Seed registration)

認証シード(Authentication Seed):

H884J5VW1ZC1E1E1

認証コード確認(Confirmation of Authentication Code):

090795

新規生成(Create a new) 登録(Register)

「登録」を押すと設定中の認証シードが上書きされて無効になります (Current Authentication Seed will be overwritten and become invalid when 'Register' is pressed)

The Authentication Seed will not be registered to the CAS server until you click the "Register" button on the Authentication Seed Management webpage. **After you register the Authentication Seed to the Authentication Application, please remember to click the "Register" button** to register the Authentication Seed to the CAS server.

Even if you mistakenly generate a new Authentication Seed, the previous Authentication Seed will remain as long as you do not click the "Register" button. Be sure to close the Multi-Factor Authentication CAS Authentication Seed Management webpage without clicking the "Register" button.

Procedures to register an Authentication Seed to Microsoft Authenticator

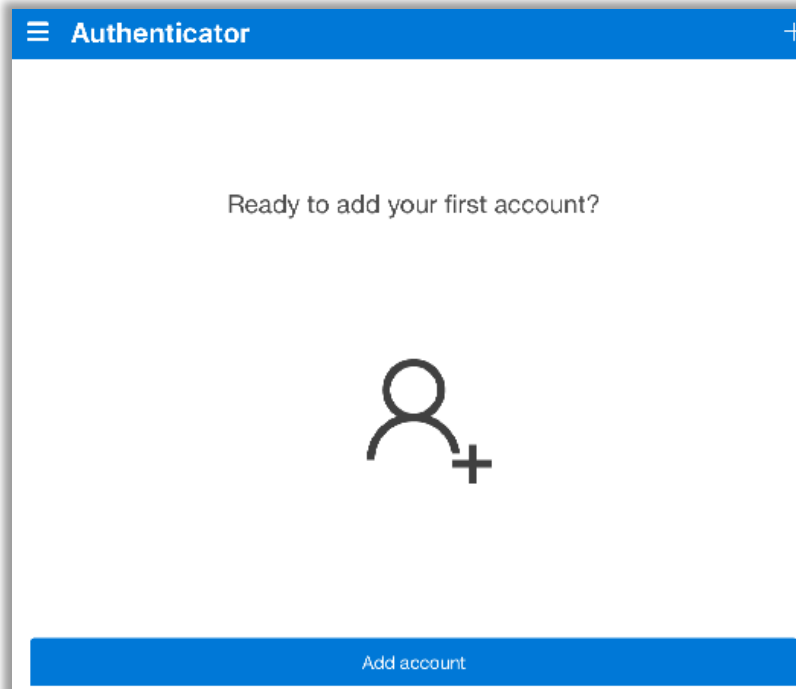
For first-time users of Microsoft Authenticator

When you open Microsoft Authenticator, it will ask for your permission to collect your data. As there is no other choice, tap "Agree" and proceed. (We highly recommend that you stop this data collection afterwards by disabling "Data for Usage Status (For improving app functionality...)" from the log menu in the App Configurations.)

Microsoft Authenticator will ask you to sign in to your Microsoft Account. Choose "Scan QR code". It is up to you whether you sign in or not.

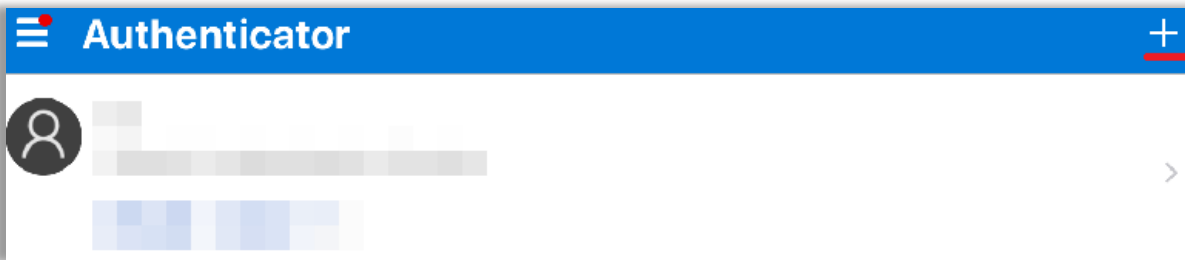
Microsoft Authenticator will proceed to the QR code scan screen.

You will receive the notification "Authenticator requires permission to use your camera" on your smartphone. Allow it.

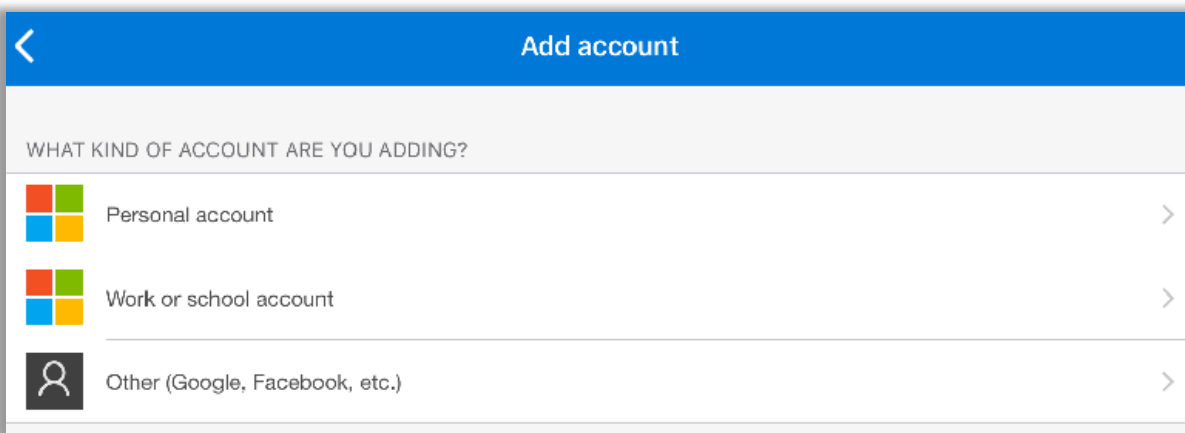


For people already using Microsoft Authenticator

After starting Microsoft Authenticator, tap the "+" mark on the upper right-hand corner, and register a new Authentication Seed.



Microsoft Authenticator will ask you to choose the service which will use multi-factor authentication. Choose "Other (Google, Facebook, etc.)".

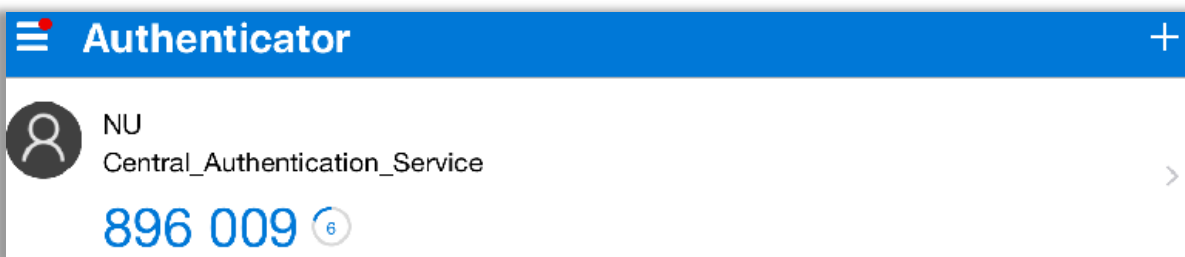


Authentication Seed registration with a QR code

Scan the QR code displayed on the Authentication Seed management webpage through QR code scan screen. The Authentication Seed will be registered as "NU (Central_Authentication_Service)"

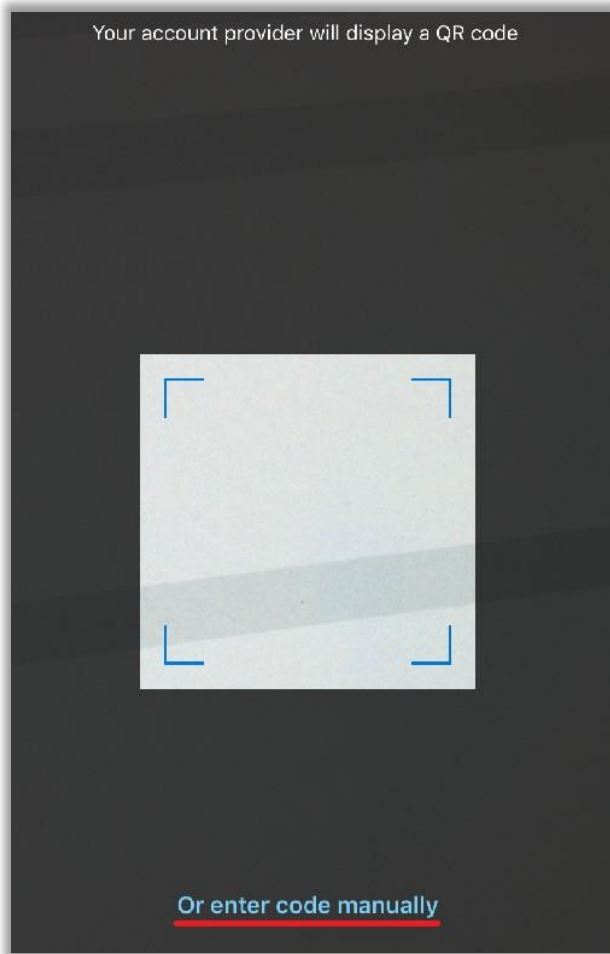
Confirm that the 6-digit number displayed in the "Confirmation of Authentication Code" field on the management webpage is the same as the one shown on Microsoft Authenticator. If they are not the same, the time on your device may be greatly out of sync.

After confirming that the 6-digit number displayed in the "Confirmation of Authentication Code" field is the same as the one shown on Microsoft Authenticator, **please remember to click the "Register" button on the Multi-Factor Authentication CAS Authentication Seed Management webpage** and register your Authentication Seed to the CAS server.



Authentication Seed registration by manually inputting the Authentication Seed (Code)

On the camera screen to scan the QR code, choose "or enter code manually".



The following Code (Authentication Seed) input screen will be shown.

- Set an "Account name" that you can remember.
- Do not use an account name that is easily identifiable as being connected to your Nagoya University ID. Input your "Authentication Seed" in the "Secret key" field.
- The authentication is not case sensitive, so you may input alphabetic characters in lower case letters if you wish. "0" (zero) and "1" (one) are not included in the codes. Please be sure to input the alphabetical "O" and "I".

A screenshot of a mobile application screen titled "Add account". It has a blue header with a back arrow on the left. Below the header, there is a section labeled "OTHER ACCOUNT". Under this section, there are two input fields: "Account name" and "Secret key". At the bottom of the screen, there is a grey button labeled "Finish".

Confirm that the 6-digit number displayed in the "Confirmation of Authentication Code" field on the management webpage is the same as the one shown on Microsoft Authenticator.

If they are not the same, the time on your device may be greatly out of sync.

After confirming that the 6-digit number displayed in the "Confirmation of Authentication Code" field is the same as the one shown on Microsoft Authenticator, **please remember to click the "Register" button on the Multi-Factor Authentication CAS Authentication Seed Management webpage** and register your Authentication Seed to the CAS server.

Trial Run of Multi-Factor Authentication CAS

We have prepared a [Multi-Factor Authentication CAS Trial webpage](#) to carry out a trial run of the Multi-Factor Authentication CAS. Following the instructions on the [Trial Run of Multi-Factor Authentication CAS webpage](#).

Authentication Seed Registration to WinAuth (Windows App)

Downloading WinAuth

Go to the [WinAuth download page](https://winauth.github.io/winauth/download.html) and download the latest version, WinAuth 3.5.1.



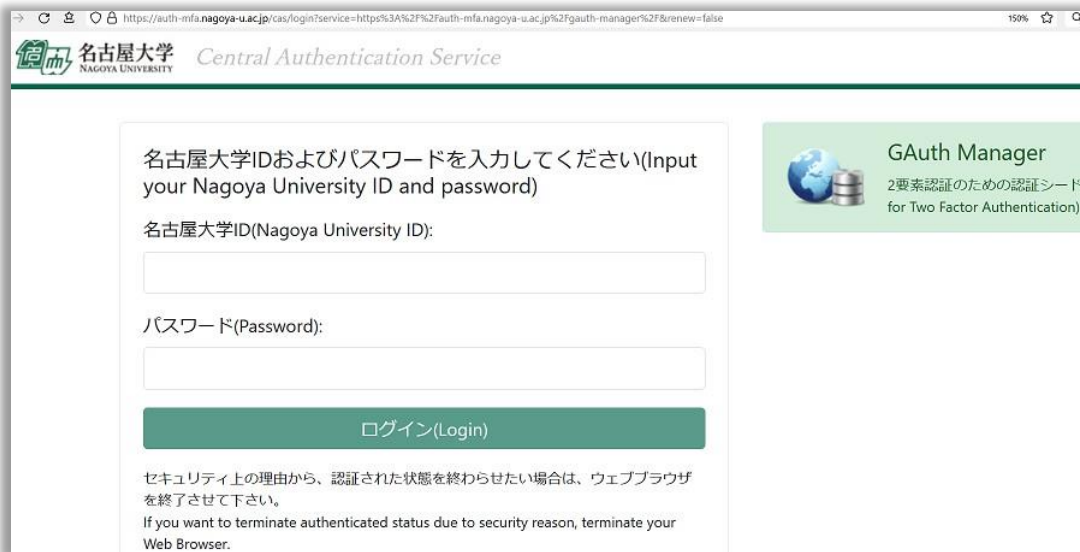
The downloaded file is in a compressed ZIP format, so decompress the file and extract WinAuth.exe.



WinAuth requires .NET Framework 4.5. Please download and install it from the Microsoft website if necessary.

Login to Authentication Seed management web page and seed generation

When you connected to [Authentication Seed management web page for Multi-Factor Authentication CAS](#), the system requires you an authentication with Nagoya University ID and password. You have to input them to authenticate.



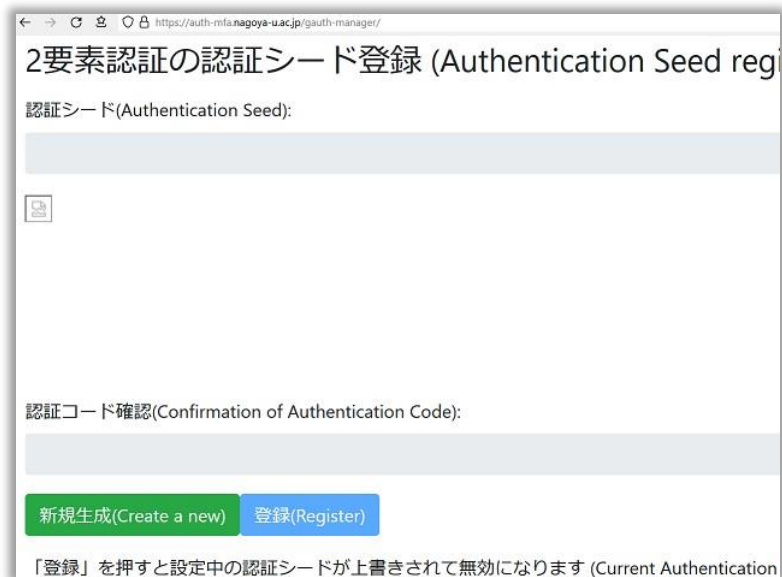
The screenshot shows the Nagoya University Central Authentication Service login page. The header includes the Nagoya University logo and the text "Central Authentication Service". The main content area has a login form with the following elements:

- Instruction: "名古屋大学IDおよびパスワードを入力してください(Input your Nagoya University ID and password)"
- Label: "名古屋大学ID(Nagoya University ID):" followed by a text input field.
- Label: "パスワード(Password):" followed by a password input field.
- A green "ログイン(Login)" button.
- A security notice: "セキュリティ上の理由から、認証された状態を終わらせたい場合は、ウェブブラウザを終了させて下さい。 If you want to terminate authenticated status due to security reason, terminate your Web Browser."

On the right side, there is a "GAuth Manager" section with a globe icon and the text "2要素認証のための認証シード登録 (Authentication Seed registration for Two Factor Authentication)".

If you push "Newly generation" button, Authentication Seed is newly generated.

You cannot see the Authentication Seed in past time again. As similar to generic password reset procedure, we only allow newly generation of Authentication Seed.



The screenshot shows the "2要素認証の認証シード登録 (Authentication Seed registration)" page. The page has the following elements:

- Section title: "2要素認証の認証シード登録 (Authentication Seed registration)"
- Label: "認証シード(Authentication Seed):" followed by a large text input field.
- Label: "認証コード確認(Confirmation of Authentication Code):" followed by a text input field.
- Two buttons: "新規生成(Create a new)" in green and "登録(Register)" in blue.
- Footer note: "「登録」を押すと設定中の認証シードが上書きされて無効になります (Current Authentication Seed will be overwritten and become invalid when you press 'Register')."

A generated Authentication Seed are presented as both "Authentication Seed (notated with alphabets and numbers)" and "QR code".



2要素認証の認証シード登録 (Authentication Seed Registration)

認証シード(Authentication Seed):

090795

QRコード

認証コード確認(Confirmation of Authentication Code):

090795

新規生成(Create a new) 登録(Register)

「登録」を押すと設定中の認証シードが上書きされて無効になります (Current Authentication Seed will be overwritten and become invalid when you push 'Register')

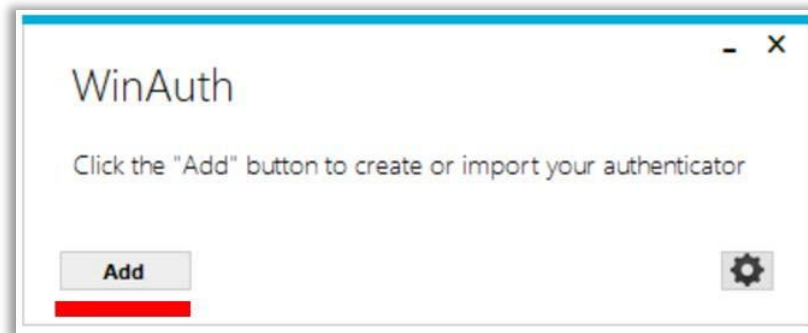
The Authentication Seed will not be registered to the CAS server until you push "Register" button. **After you register Authentication Seed to Authentication Application, push "Register" button to register Authentication Seed to CAS server.**

If you wrongly generated a new Authentication Seed, the Authentication Seed from past times are still existing if you do not push "Register" button. Close the Authentication Seed management web page without pushing "Register" button.

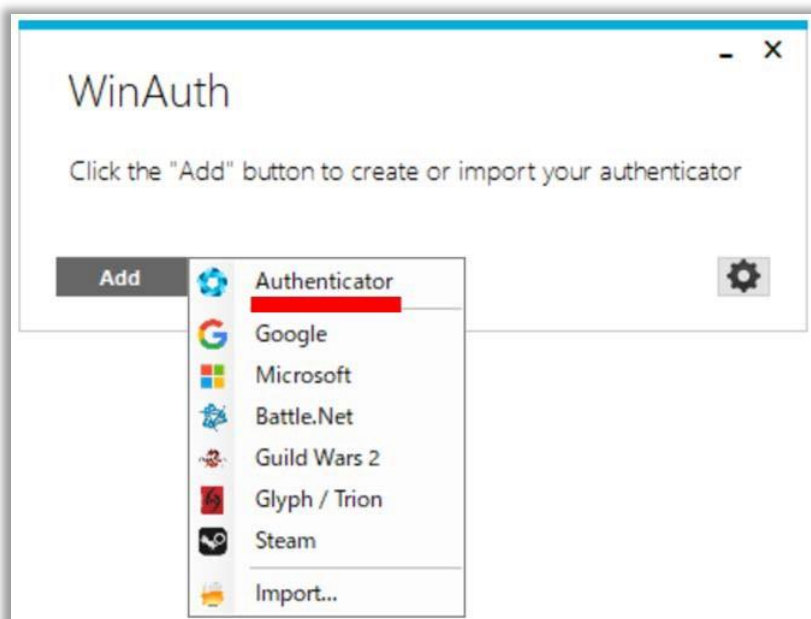
Authentication Seed registration to WinAuth

You will be asked to register an Authentication Seed the first time you start WinAuth.

Click "Add" and proceed with the Authentication Seed registration. Those who are already using WinAuth can also proceed with the Authentication Seed registration by choosing "Add" from a different screen.



You will see a selection screen that asks you to choose the service which will use multi-factor authentication, but as Nagoya University CAS is not included in the options, please choose "Authenticator" at the top of the list.



Input a service name (Name field), Authentication Seed value (1.), and Authentication Seed generation method (2.). For the service name (Name field), you can input any name you want to register for.

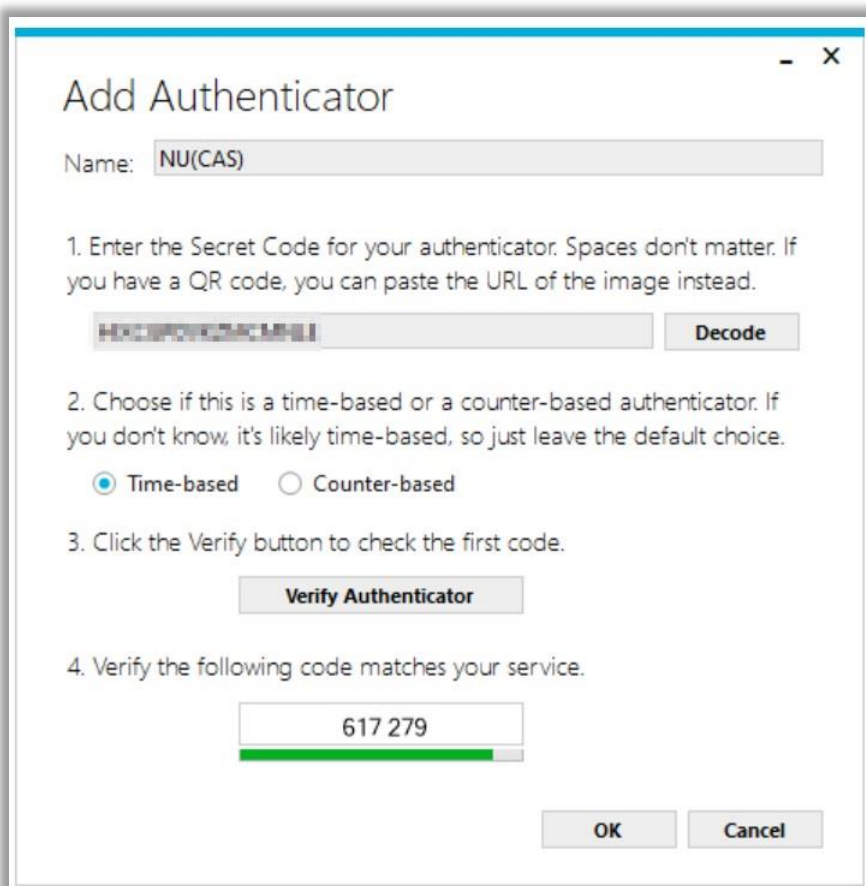
**However, please avoid inputting your Nagoya University ID as it is used for generating Authentication Seed value.
For the Authentication Seed value (1.), please input your "Authentication Seed" displayed on the Multi-Factor Authentication CAS Authentication Seed Management webpage.
For the Authentication Seed generation method (2.), please choose "Time-based".**

If you click "Verify Authenticator" (3.), the 6-digit number will be generated based on the Authentication Seed value and displayed in (4.).

Confirm that the 6-digit number displayed in the "Confirmation of Authentication Code" field on the Multi-Factor Authentication CAS Authentication Seed Management webpage is the same as the one shown on WinAuth.

If they are the same, click on "OK".

they are not the same, the time on your device may be greatly out of sync.



The image shows the 'Add Authenticator' window from the WinAuth application. It has a title bar with standard Windows window controls. The main content area is titled 'Add Authenticator'. Below the title, there is a text field labeled 'Name:' containing the text 'NU(CAS)'. Below this, there are four numbered instructions: 1. Enter the Secret Code for your authenticator. Spaces don't matter. If you have a QR code, you can paste the URL of the image instead. 2. Choose if this is a time-based or a counter-based authenticator. If you don't know, it's likely time-based, so just leave the default choice. 3. Click the Verify button to check the first code. 4. Verify the following code matches your service. Following these instructions, there is a text input field containing the code '617 279'. Below the input field is a green progress bar. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

Name: NU(CAS)

1. Enter the Secret Code for your authenticator. Spaces don't matter. If you have a QR code, you can paste the URL of the image instead.

2. Choose if this is a time-based or a counter-based authenticator. If you don't know, it's likely time-based, so just leave the default choice.

☒ Time-based ☐ Counter-based

3. Click the Verify button to check the first code.

4. Verify the following code matches your service.

617 279

OK Cancel



The image shows a web browser window displaying the '2要素認証の認証シード登録 (Authentication Seed Management)' page. The address bar shows the URL 'https://auth-mfa.nagoya-u.ac.jp/gauth-manager/'. The page title is '2要素認証の認証シード登録 (Authentication Seed Management)'. Below the title, there is a section labeled '認証シード(Authentication Seed):' with a text input field containing a QR code. Below this, there is a section labeled '認証コード確認(Confirmation of Authentication Code):' with a text input field containing the code '090795'. At the bottom, there are two buttons: '新規生成(Create a new)' and '登録(Register)'. A footer note at the bottom states: '「登録」を押すと設定中の認証シードが上書きされて無効になります (Current Authentication Seed will be overwritten and become invalid when you press 'Register').'

2要素認証の認証シード登録 (Authentication Seed Management)

認証シード(Authentication Seed):

090795

新規生成(Create a new) 登録(Register)

「登録」を押すと設定中の認証シードが上書きされて無効になります (Current Authentication Seed will be overwritten and become invalid when you press 'Register').

The next step is to set the protection settings for WinAuth.

- In the "Protect with my own Password" field, you can set a password that will be required to open WinAuth.
- Set your password by inputting it in the "Password" field and confirm your password by inputting it again in the "Verify" field. Make sure to input the different password from the one used for your Nagoya University ID.
- By enabling "Encrypt to only be useable on this computer" and "And only by the current user on this computer", you can prevent people with malicious intent from copying the password and using it on other computers.

The screenshot shows the 'Protection' window of WinAuth. It has a title bar with standard Windows window controls. The main heading is 'Protection'. Below it, a paragraph explains that users should select how to protect their authenticators, with a note that using a password is strongly recommended. There are three main sections: 1. 'Protect with my own password' (checked): Includes a description that authenticators will be encrypted with the user's password and will be inaccessible if forgotten without a backup. It features two password input fields labeled 'Password' and 'Verify', both containing masked characters. 2. 'Additionally, you can protect and encrypt your data using the built-in Windows account encryption. This will lock your authenticators to this computer or user so they cannot be opened even if the files are copied. You MUST turn this off if you are going to reformat your disk, re-install Windows or delete this user account.' This section contains two checked checkboxes: 'Encrypt to only be useable on this computer' and 'And only by the current user on this computer'. 3. 'Lock with a YubiKey' (unchecked): Includes a description that the YubiKey must support Challenge-Response using HMAC-SHA1. It shows a 'Slot' selection with '1' chosen and a corresponding YubiKey icon. Below this are 'Use Slot' and 'Configure Slot' buttons. At the bottom right, there are 'OK' and 'Cancel' buttons.

Protection

Select how you would like to protect your authenticators. Using a password is strongly recommended, otherwise your data could be read and stolen by malware running on your computer.

☒ Protect with my own password

Your authenticators will be encrypted using your own password and you will need to enter your password to open WinAuth. Your authenticators will be inaccessible if you forget your password and you do not have a backup.

Password: [masked]

Verify: [masked]

Additionally, you can protect and encrypt your data using the built-in Windows account encryption. This will lock your authenticators to this computer or user so they cannot be opened even if the files are copied. You MUST turn this off if you are going to reformat your disk, re-install Windows or delete this user account.

☒ Encrypt to only be useable on this computer

☒ And only by the current user on this computer

☐ Lock with a YubiKey

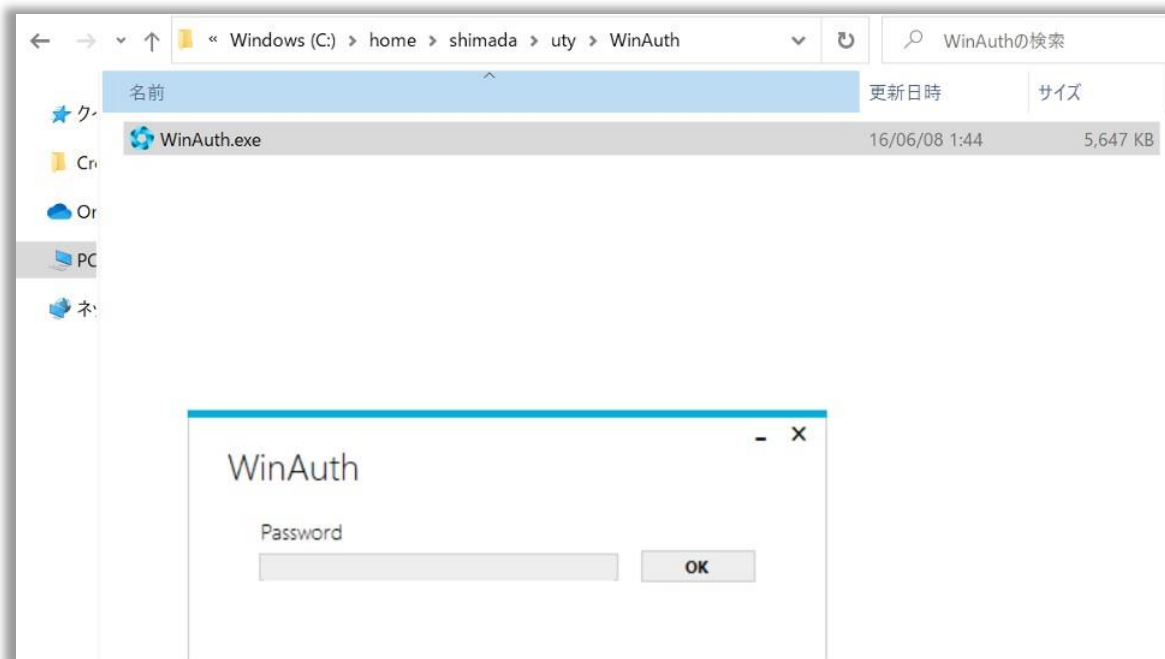
Your YubiKey must support Challenge-Response using HMAC-SHA1 in one of its slots. Use the YubiKey personalization tool to configure the slot or click the Configure Slot button.

Slot: 1 [YubiKey icon]

Use Slot Configure Slot

OK Cancel

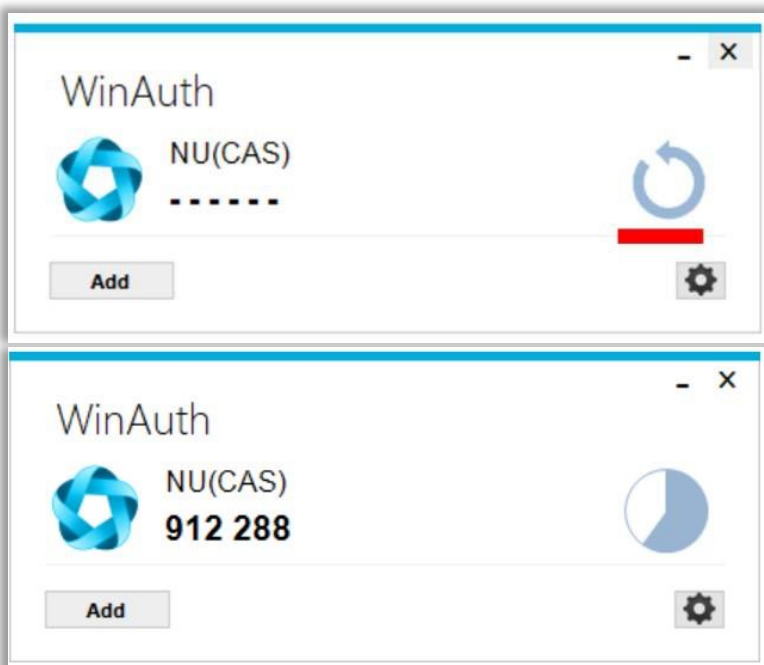
Use of WinAuth



Double click to open WinAuth.exe. If you have set a password, you will be prompted to enter it.

The 6-digit number required for each service's multi-factor authentication will be displayed.

Note that it will only be displayed if you click on the refresh mark on the right-hand side of each service name.



After confirming that the 6-digit number displayed in the "Confirmation of Authentication Code" field is the same as the one shown on WinAuth, please remember to click the "Register" button on the Multi-Factor Authentication CAS Authentication Seed Management webpage and register your Authentication Seed to the CAS server.

Q&A about WinAuth

Q: I forgot the password set for WinAuth.

A: Delete the files in the following location. However, please note that doing so will also reset all settings for WinAuth, including the Authentication Seed.

C:¥Users(Your_User_Name)¥AppData¥Roaming¥WinAuth¥winauth.xmlbr>

Trial Run of Multi-Factor Authentication CAS

We have prepared a [Multi-Factor Authentication CAS Trial webpage](#) to carry out a trial run of the Multi-Factor Authentication CAS. Following the instructions on the [Trial Run of Multi-Factor Authentication CAS webpage](#).

Authentication Seed Registration to Step Two (macOS App)

Downloading Step Two

Go to the [Step Two page of Mac App Store](#) and download the latest version.



Login to the Authentication Seed Management webpage and Authentication Seed generation

When you connect to the [Multi-Factor Authentication CAS Authentication Seed Management webpage](#), the system requires authentication with your Nagoya University ID and password, so please input them to authenticate.

To distribute Authentication Seeds safely, access to the Authentication Seed Management webpage is only allowed from the Nagoya University's network on campus excluding special case.

A screenshot of the Nagoya University Central Authentication Service login page. The page has a header with the Nagoya University logo and 'Central Authentication Service'. The main content area has a form with the text '名古屋大学IDおよびパスワードを入力してください(Input your Nagoya University ID and password)'. Below this are two input fields: '名古屋大学ID(Nagoya University ID):' and 'パスワード(Password):'. A green 'ログイン(Login)' button is at the bottom of the form. To the right of the form is a green box titled 'GAuth Manager' with a globe icon and text '2要素認証のための認証シード (for Two Factor Authentication)'. At the bottom of the page, there is a security notice in Japanese and English: 'セキュリティ上の理由から、認証された状態を終わらせたい場合は、ウェブブラウザを終了して下さい。 If you want to terminate authenticated status due to security reason, terminate your Web Browser.'

If you click the "Create a new" button, a new Authentication Seed will be generated.



You cannot display a previously used Authentication Seed. Similar to other password reset procedures, you can only generate and register a new Authentication Seed.

The generated Authentication Seed will be displayed as both an "Authentication Seed" (consisting of alphanumeric characters) and a "QR code".



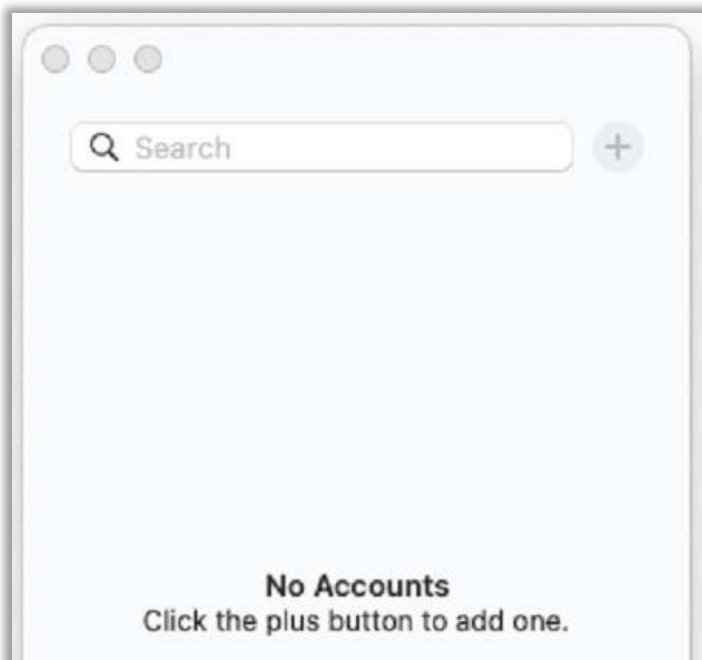
The Authentication Seed will not be registered to the CAS server until you click the "Register" button on the Authentication Seed Management webpage. **After you register the Authentication Seed to the Authentication Application, please remember to click the "Register" button** to register the Authentication Seed to the CAS server.

Even if you mistakenly generate a new Authentication Seed, the previous Authentication Seed will remain as long as you do not click the "Register" button. Be sure to close the Multi-Factor Authentication CAS Authentication Seed Management webpage without clicking the "Register" button

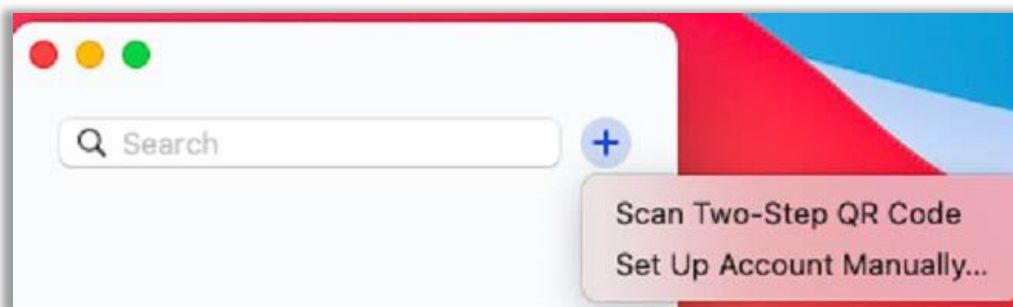
Authentication Seed registration to Step Two (with QR code)

You will be asked to register an Authentication Seed the first time you start Step Two.

Click "+ Button" and proceed with the Authentication Seed registration. Those who are already using Step Two can also proceed with the Authentication Seed registration by choosing "+ Button".



After you push "+ Button", Step Two asks you to Authentication Seed registration method. Choose "Scan Two-Step QR Code".



A window for QR code scan rises. Put the window to QR code on the web browser.

2要素認証の認証シード登録 (Authentication Two Factor Authentication)

認証シード (Authentication Seed):

HR2UWZJQM5ZDK3ZX

QR Code Scanner

認証コード確認 (Confirmation of Authentication Code):

667074

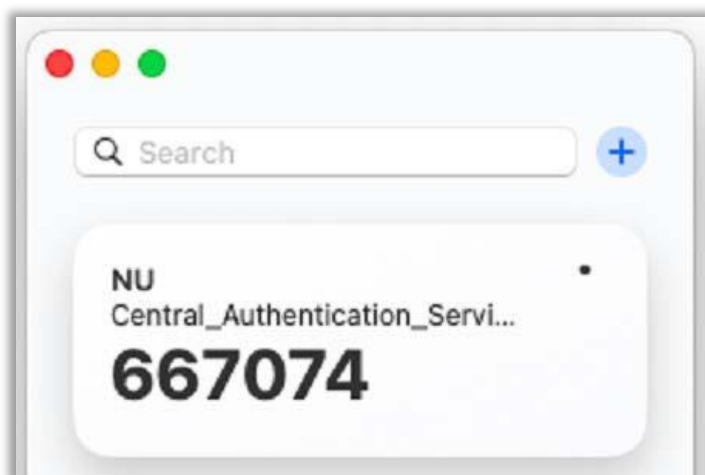
新規生成 (Create a new) 登録 (Register)

「登録」を押すと設定中の認証シードが上書きされて無効になります (Current and invalidated if you push "Register" button)

The Authentication Seed is registered to Step Two and Step Two displays Service Name and Authentication Code pair.

Confirm that the 6-digit number displayed in the "Confirmation of Authentication Code" field on the Multi-Factor Authentication CAS Authentication Seed Management webpage is the same as the one shown on Step Two.

If they are not the same, the time on your device may be greatly out of sync.

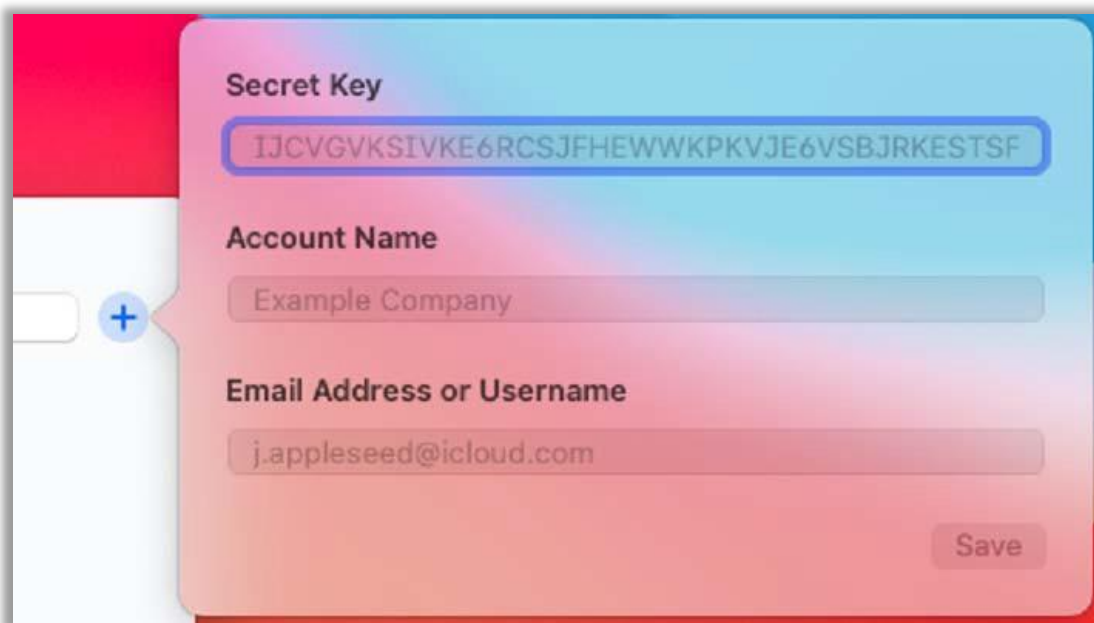


Authentication Seed Registration with alphanumeric Authentication Seed

If your environment cannot accept QR code with some reason, you can choose Authentication Seed registration with alphanumeric Authentication Seed.

Choose "Set Up Account Manually" at Authentication Seed registration selection.

- Input Authentication Code to "Secret Key" item.
- Input proper (identifiable) "Account Name" and "Email Address or Username" with yourself. Note that we recommend you to avoid your Nagoya University ID and mail address of Nagoya University Mail Service directly to avoid vulnerability of peeping.
- Confirm Authentication Code on Step Two and Authentication Code on the web page are identical.
- If they are not the same, the time on your device may be greatly out of sync.



The image shows a mobile application interface for registering an authentication seed. It features a light blue header with the title "Secret Key". Below this is a text input field containing the alphanumeric string "IJC VG VKSIVKE6RCSJFHEWWKPKVJE6VSBJRKESTSF". The next section is titled "Account Name" and has a text input field with the placeholder text "Example Company". Below that is the "Email Address or Username" section with a text input field containing "j.appleseed@icloud.com". A "Save" button is located at the bottom right of the form. The interface has a clean, modern design with a white background and blue accents.

Trial Run of Multi-Factor Authentication CAS

We have prepared a [Multi-Factor Authentication CAS Trial webpage](#) to carry out a trial run of the Multi-Factor Authentication CAS. Following the instructions on the [Trial Run of Multi-Factor Authentication CAS webpage](#).

Question and Answer for Multi-Factor Authentication CAS

Q: May I register Authentication Seed to multiple devices?

A: Yes. For convenience, you can register Authentication Seed to multiple devices (e.g. both smartphone and PC) if you can guarantee security.

Q: I obtained a new smartphone. However, I forgot to do the migration procedures for the Authentication Application on my smartphone.

A: As shown in the [Authentication Seed Registration to the Authentication Application](#) webpage, you have to create a new Authentication Seed by accessing the Multi-Factor Authentication CAS Authentication Seed Registration webpage from within the University.

The previous Authentication Seed becomes invalid after registering a new Authentication Seed..

Q: May I use the cloud backup feature on the Authentication Application on my smartphone?

A: If you are using a reliable Authentication Application, you can use the cloud backup feature.

Q: I lost my smartphone, and want to register an Authentication Seed to my new smartphone.

A: As shown in the [Authentication Seed Registration to the Authentication Application](#) webpage, you have to create a new Authentication Seed by accessing the Multi-Factor Authentication CAS Authentication Seed Registration webpage from within the University.

The previous Authentication Seed becomes invalid after registering a new Authentication Seed..

Q: I lost my hardware token, so I want to disable it as soon as possible.

A: Please go to the [IT Help Desk](#) with your staff/student ID card and submit a request to disable your hardware token.

Q: I want to register a new hardware token.

A: Follow the procedures for [Registration of Hardware Token](#), and register the new hardware token. Note that after registration is complete, the previous hardware token will be disabled.

Q: I want to know more about the Multi-Factor Authentication.

A: We have a webpage dedicated to [Tips regarding Multi-Factor Authentication](#).

Trial Run of Multi-Factor Authentication CAS

We have prepared a [Multi-Factor Authentication CAS Trial webpage](#) to carry out a trial run of the Multi-Factor Authentication CAS.

Trial Run Procedures

When you access the [Multi-Factor Authentication CAS Authentication Trial webpage](#), the CAS system requires you to input your Nagoya University ID and password.

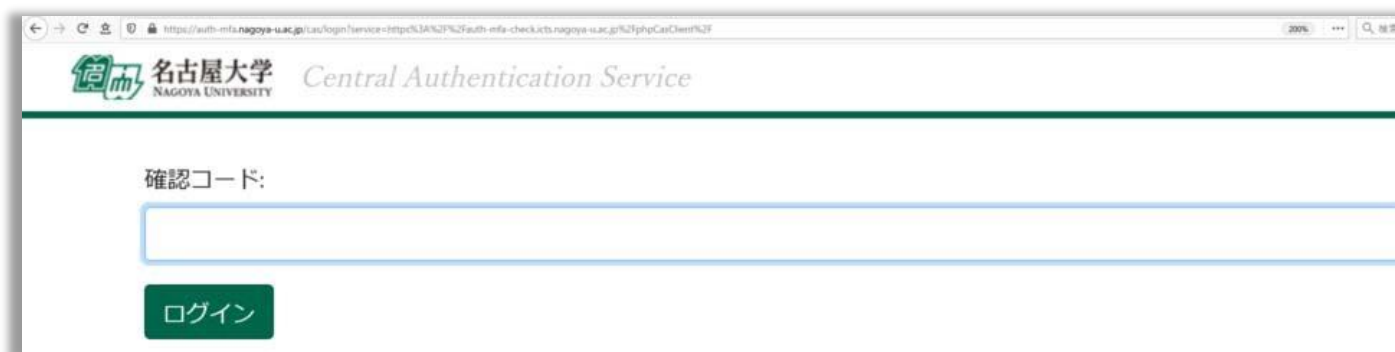
If the CAS system has already memorized your Nagoya University ID and password, the CAS system will start at the second step that asks to input an Authentication Code (6-digit number).



The screenshot shows a web browser window displaying the Nagoya University Central Authentication Service (CAS) login page. The page title is "名古屋大学 Central Authentication Service". The main heading is "名古屋大学IDおよびパスワードを入力してください" (Please enter your Nagoya University ID and password). Below this, there are two input fields: "名古屋大学ID:" and "パスワード:". A green "ログイン" (Login) button is positioned below the password field. To the right of the login form, there is a green box with a globe icon and the text "MFAチェックサイト". At the bottom of the login form, there is a security notice in Japanese: "セキュリティ上の理由から、認証が必要なサービスのアクセス終了時には、ウェブブラウザをログアウトし、終了してください" (For security reasons, when the access to the service requiring authentication ends, please log out of the web browser and end the session).

After you enter a valid Nagoya University ID and password, the CAS system will ask you to input an Authentication Code (6-digit number) as the second factor.

Input the Authentication Code presented on the Authentication Application or hardware token. The CAS system will also accept the Authentication Codes from the previous or subsequent interval, so you can proceed with authentication even if the Authentication Code changes during the authentication process.



The screenshot shows the Nagoya University Central Authentication Service login page. At the top, there is a header with the Nagoya University logo and the text "Central Authentication Service". Below the header, there is a label "確認コード:" (Confirmation Code:). Underneath the label is a text input field. Below the input field is a green button labeled "ログイン" (Login).

If authentication using the Authorization Code is successful, the webpage indicating successful authentication will appear.

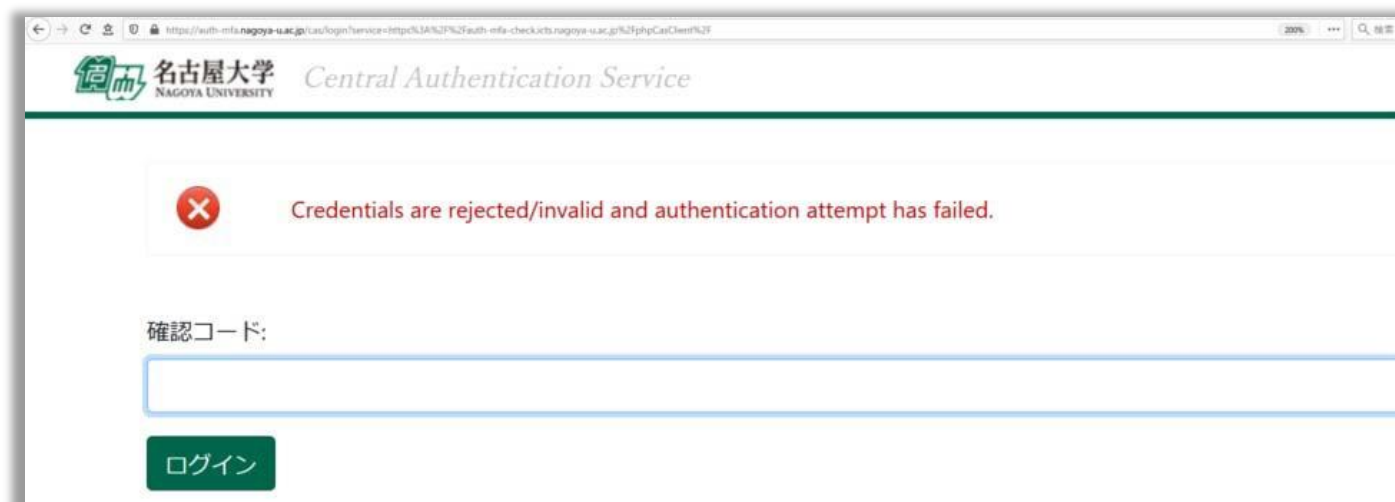


The screenshot shows the Nagoya University Central Authentication Service successful authentication page. At the top, there is a header with the Nagoya University logo and the text "Central Authentication Service". Below the header, there is a large green banner with the text "認証成功。多要素認証CAS利用OKです。" (Authentication successful. Multi-factor authentication CAS use OK). Below the banner, there is a link labeled "Logout".

This concludes the trial run, so you may close the webpage.

If the authentication was unsuccessful, the webpage indicating an unsuccessful authentication will appear. Input the Authentication Code presented on the Authentication Application or hardware token again.

See "If you are having trouble with authentication" below if you are having repeated unsuccessful attempts.



The screenshot shows the Nagoya University Central Authentication Service unsuccessful authentication page. At the top, there is a header with the Nagoya University logo and the text "Central Authentication Service". Below the header, there is a red error message box with a red 'X' icon and the text "Credentials are rejected/invalid and authentication attempt has failed." Below the error message, there is a label "確認コード:" (Confirmation Code:). Underneath the label is a text input field. Below the input field is a green button labeled "ログイン" (Login).

If you are having trouble with authentication

The clock of the device you are running the Authentication Application on is incorrect.

- > Change the clock on your device to the correct time. You have registered the wrong Authentication Seed.
- > Start over from the [Authentication Seed registration](#).

The clock of the hardware token is greatly out of sync.

- > Apply for hardware token use again and let us know about your issue when registering.

Application to Use Hardware Token for Multi- Factor Authentication CAS

If you wish to use a hardware token, you will need to purchase a hardware token using departmental budgets etc., in addition to registering the hardware token to the Multi-Factor Authentication CAS.

Obtaining a hardware token

The hardware tokens that can be used for the Multi-Factor Authentication CAS are those that are “OATH-TOTP standard with 30 second update intervals that output 6-digit authentication codes”.

The manufacturer of the hardware token does not matter if these specifications are met.

In order to register a hardware token to the Multi-Factor Authentication CAS, the Authentication Seed that is pre-encoded into the hardware token is required. Be sure that the “BASE32 Encoded Authentication Seed” that comes alongside your hardware token from the hardware token vendor is kept secure and in a safe place.

Hardware tokens that have been used are as follows. If you have any concerns regarding purchases, please contact the Multi-Factor Authentication CAS Project (multiauth@icts.). (: nagoya-u.ac.jp)

[Feitian Japan One-Time Password \(TOP\) Token](#)

Registering the Authentication Seed of your hardware token to Multi-Factor Authentication CAS

Fill out the Hardware Token Application Form below and submit it to the [IT Help Desk](#) on the first floor of the Information Technology Center. Please also bring your Staff/Student ID card so that we can verify your identity. Once Authentication Seed registration is complete, we will send an e-mail to your contact e-mail address to notify you of the Seed registration completion.

[Hardware Token Application Form on Forms \(application of Authentication Seed\)](#)

If you cannot use Forms (e.g. you do not have right to use Office 365), please fill following Word version Hardware Token Application Form and bring it to the [IT Help Desk](#) on the first floor of the Information Technology Center with your Staff/Student ID card so that we can verify your identity.

[Word version Hardware Token Application Form \(For person who cannot use Forms\)](#)

Multi-factor authentication using hardware tokens

The 6-digit number displayed when you press the button on your hardware token will be the second factor (Authentication Code) in the authentication process. Specific procedures for authentication are indicated on the [Multi-Factor Authentication CAS Trial webpage] ([./mfa_cas_authentication_test.html](#)) .



Q&A about hardware token applications

Q: I lost my hardware token, so I want to disable it as soon as possible.

A: Please go to the [IT Help Desk](#) with your Staff/Student ID card and submit a request to disable your hardware token.

Q: I want to register a new hardware token.

A: Follow the instructions indicated on this webpage and register the new hardware token. Note that after registration is complete, the previous hardware token will be disabled.

Q: I lost my hardware token, but I have to urgent matter.

A: We have few hardware tokens to lend. Please take contact to [IT Help Desk](#).