

Two-Factor Authentication Settings for IIS VPN

Edition 2024/2/29

The IIS VPN server will be replaced this winter. The new server will require two-factor authentication (2FA). Two-factor authentication must be configured before using the new VPN server (vpn1.iis.u-tokyo.ac.jp). However, the general usage is the same as the current VPN server (vpn0.iis.u-tokyo.ac.jp). Please note that 2FA is different from the IIS mail server and needs to be configured separately for VPN.

Initial setup of two-factor authentication for VPN

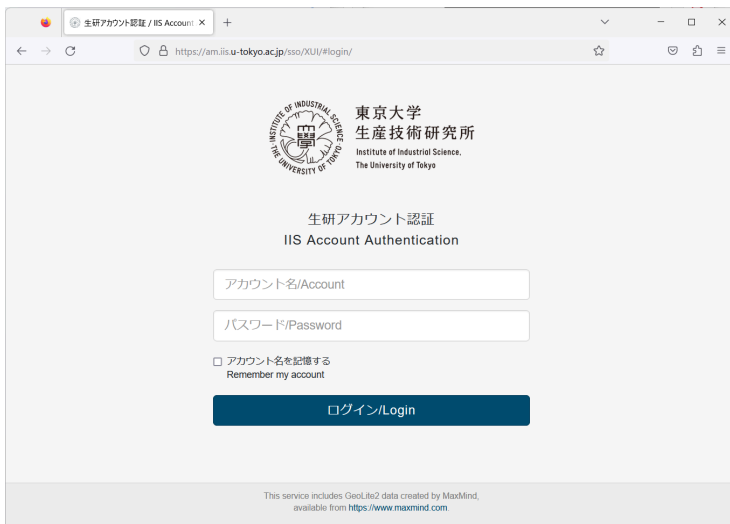
Before accessing vpn1.iis.u-tokyo.ac.jp, please configure the following settings.

Please access the following URL to setup 2FA for VPN:

<https://am.iis.u-tokyo.ac.jp/sso/XUI/#login/&service=TOTPRegistration&ForceAuth=true>

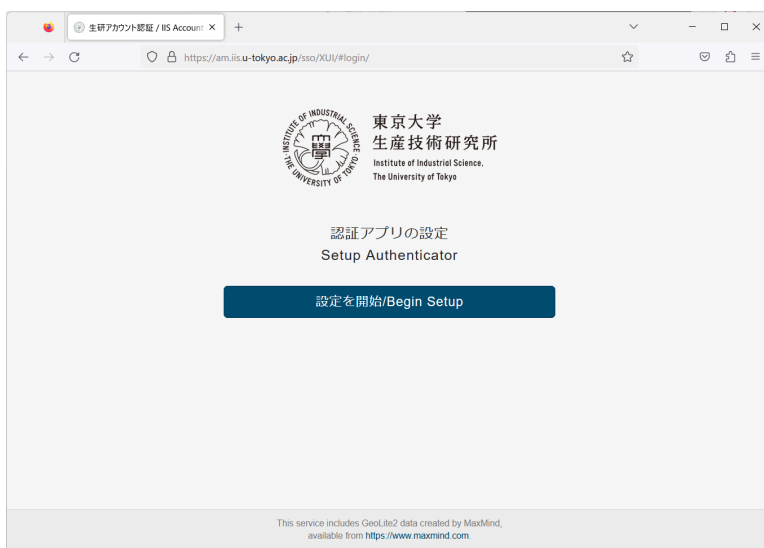
Please enter your IIS account and password.

Do not include “@iis.u-tokyo.ac.jp” in the account name because it fails.



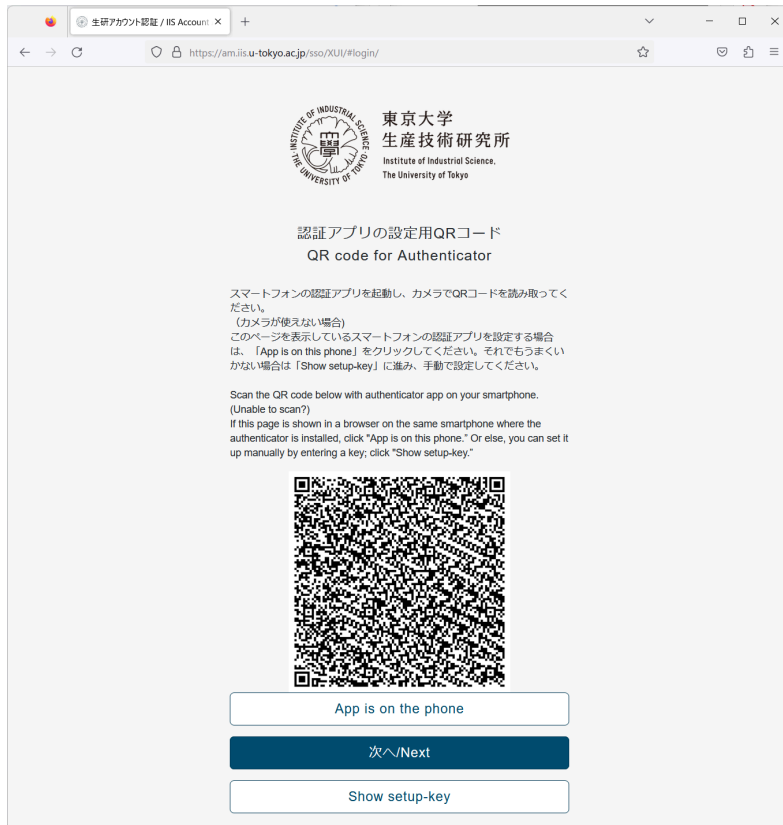
The screenshot shows a web browser window with the URL <https://am.iis.u-tokyo.ac.jp/sso/XUI/#login/>. The page header includes the logo of the Institute of Industrial Science, The University of Tokyo. The main content area is titled "生研アカウント認証" (IIS Account Authentication) and contains two input fields: "アカウント名/Account" and "パスワード/Password". Below the fields is a checkbox labeled "アカウント名を記憶する" (Remember my account). A blue button labeled "ログイン/Login" is positioned below the checkbox. At the bottom of the page, there is a small disclaimer: "This service includes Geolite2 data created by MaxMind, available from https://www.maxmind.com".

After logging in, the "Setup Authenticator" screen will appear. Select "Begin Setup".



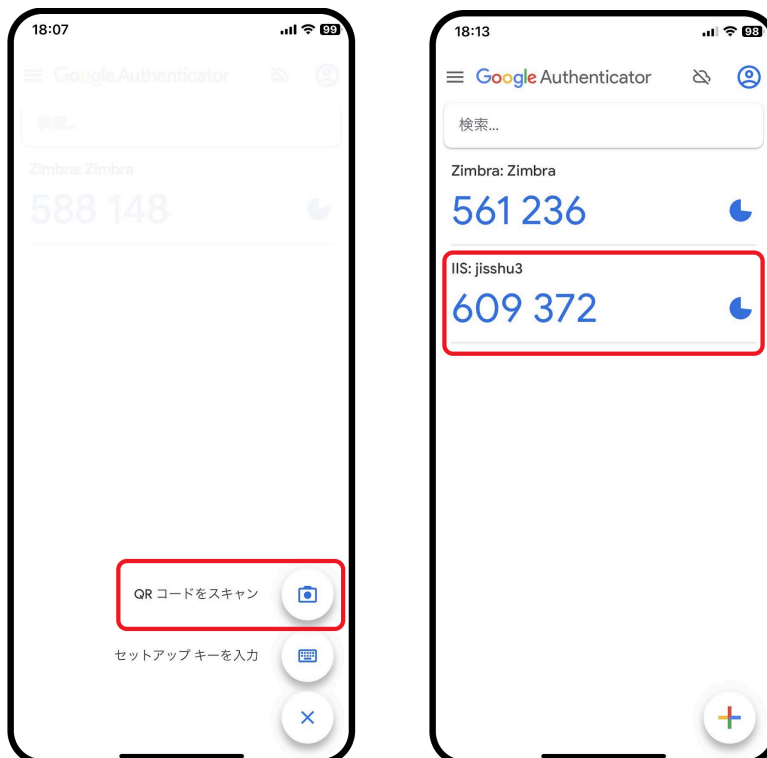
The screenshot shows the same web browser window after logging in. The page header and logo are identical. The main content area is titled "認証アプリの設定" (Setup Authenticator) and features a prominent blue button labeled "設定を開始/Begin Setup". The same disclaimer is visible at the bottom of the page.

A QR code will be displayed. Scan the QR code with Authenticator on your smartphone. The following explanation is based on the use of Google Authenticator.



1. Launch Google Authenticator on your smartphone and tap the "+" button in the lower right corner.
2. Select "Scan a QR Code" to read the QR code.

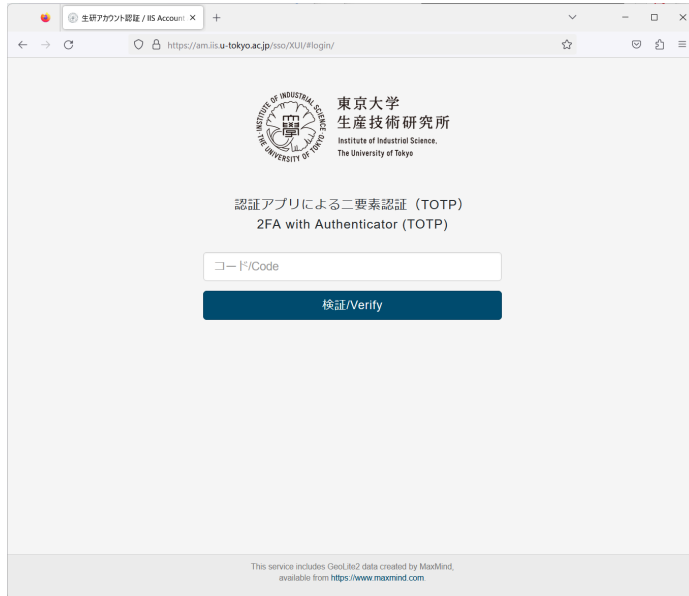
In Google Authenticator, the code will be displayed in "IIS:Account name".



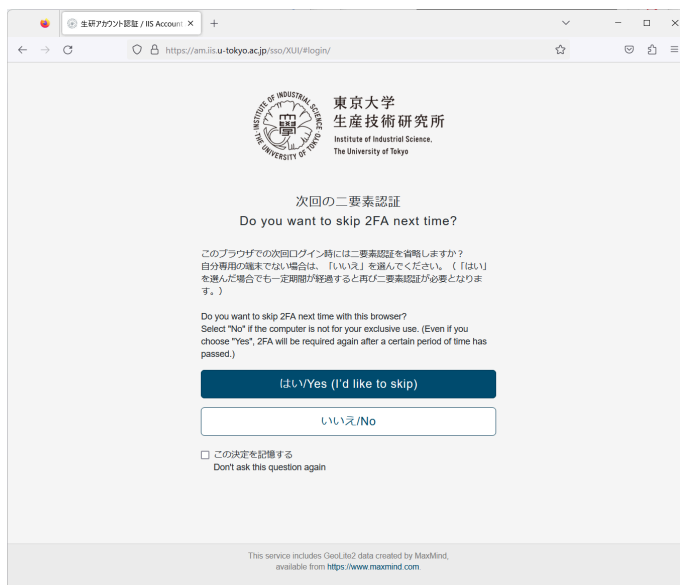
On the browser side, select "Next".

The "2FA with Authenticator (TOTP) " screen will appear.

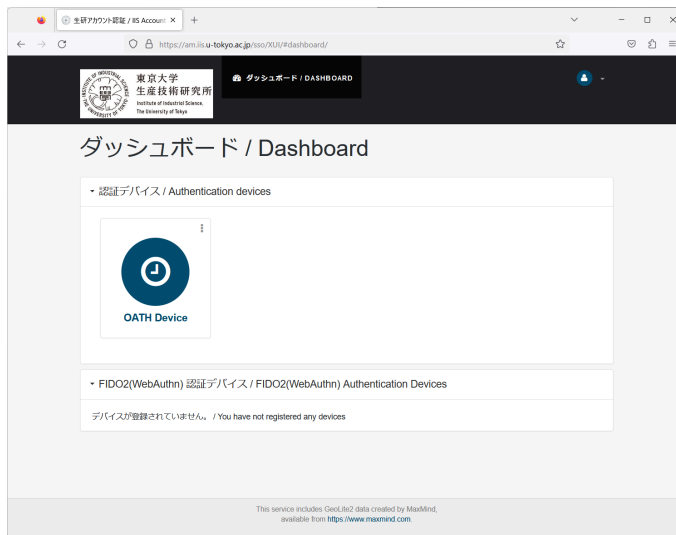
Enter the code on your smart phone and select "Verify".



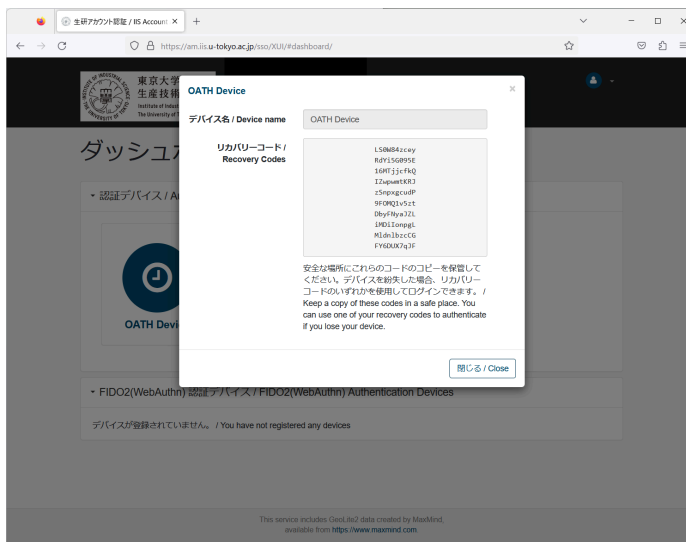
If the verification is successful, you will be taken to the screen to ask if you want to skip the next 2FA. Please select "No" for the first time.



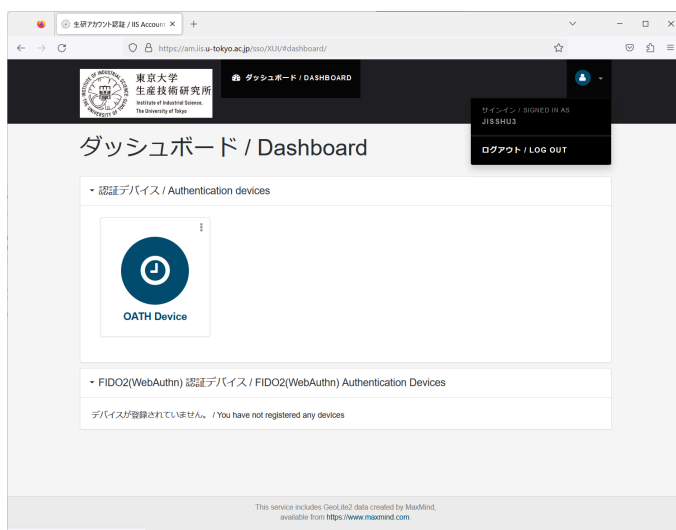
A dashboard will appear.



Select "OATH Device." Ten recovery codes will be displayed. Copy and keep them. You can also log in by entering one of the recovery codes when entering the two-factor authentication code. You will also need this code to reset the two-factor authentication due to a change of model or loss of your smartphone.



Select "Logout" from ▼ in the upper right corner. When the logout screen appears, the setup is complete.



Installing AnyConnect

If Cisco AnyConnect (Cisco Secure Client) is already installed to connect to vpn0.iis.u-tokyo.ac.jp or UTokyo VPN, this step is not necessary and you can go to “Use of VPN” on p.7.

If you have not installed AnyConnect yet, please follow the steps below.

For Android

Install Cisco Secure Client from the Google Play Store. Verify that the provider is Cisco Systems, Inc.

For Apple iOS/iPad OS

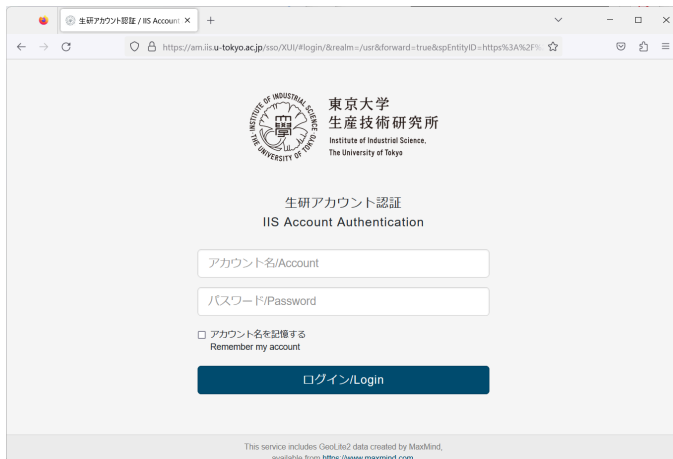
Install Cisco Secure Client from the App Store. Verify that the provider is Cisco Systems, Inc.

For Windows, macOS, and Linux

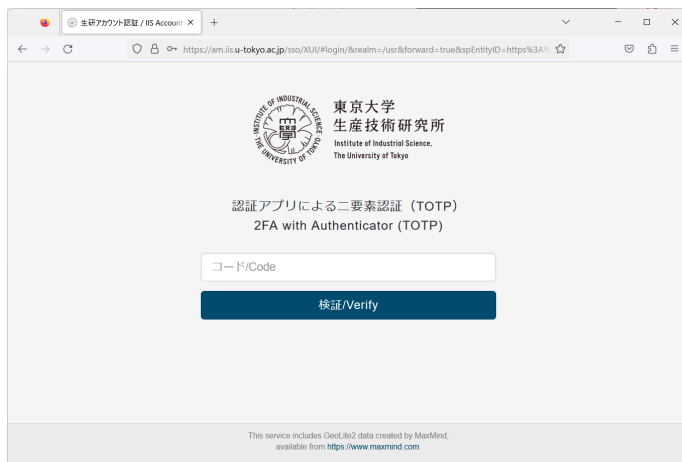
Please access the following URL:

<https://vpn1.iis.u-tokyo.ac.jp/>

Accessing the above URL will take you to the two-factor authentication screen at <https://am.iis.u-tokyo.ac.jp/sso>. Enter your IIS account (do not include “@iis.u-tokyo.ac.jp”) and password, then enter the two-factor authentication code displayed on your smartphone.

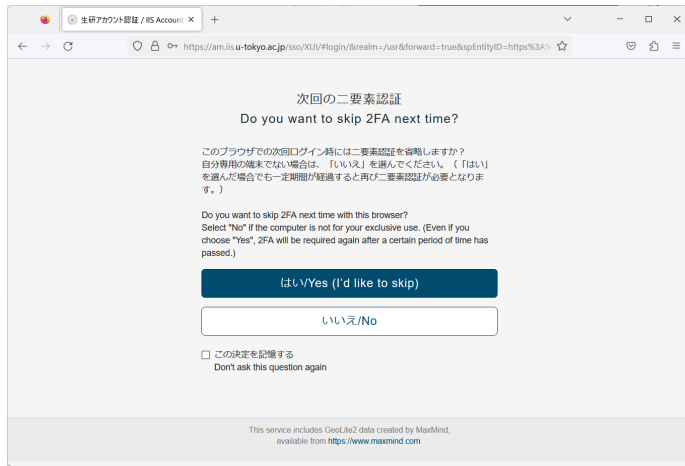


The screenshot shows a web browser window with the URL <https://am.iis.u-tokyo.ac.jp/sso/XUI/#login?realm=/usr&forward=true&spEntityID=https%3A%2F%2Fvpn1.iis.u-tokyo.ac.jp/>. The page header includes the logo of the Institute of Industrial Science, The University of Tokyo. The main heading is “生研アカウント認証 / IIS Account Authentication”. Below the heading are two input fields: “アカウント名/Account” and “パスワード/Password”. There is a checkbox labeled “アカウント名を記憶する / Remember my account”. A blue button labeled “ログイン/Login” is positioned below the fields. At the bottom of the page, there is a small disclaimer: “This service includes GeoLite2 data created by MaxMind, available from https://www.maxmind.com”.

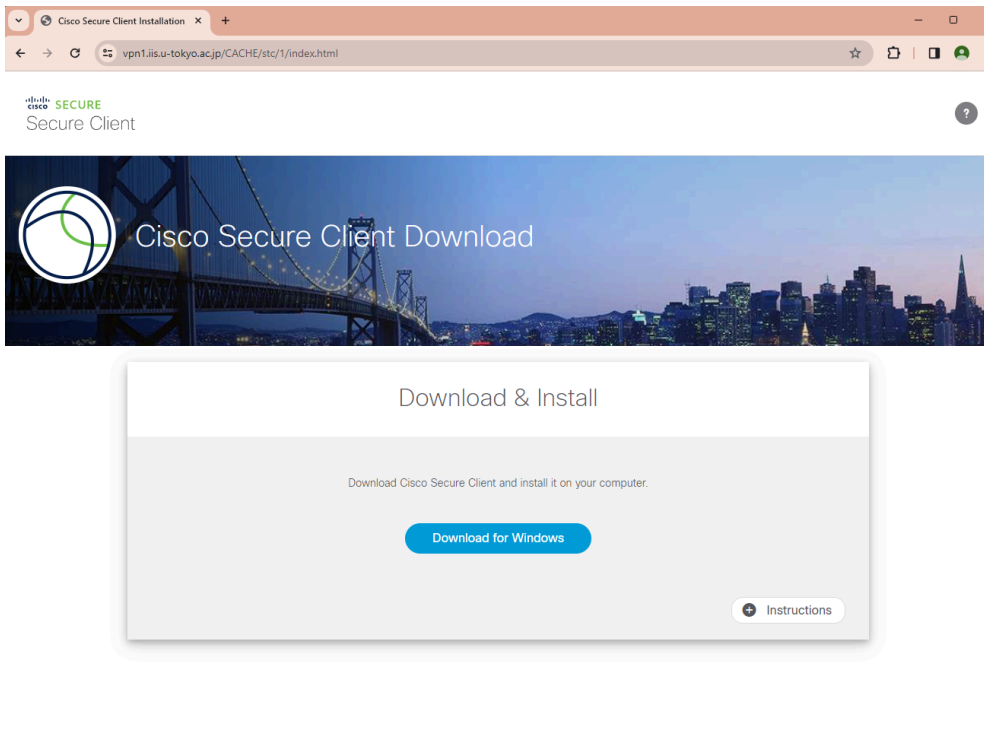


The screenshot shows a web browser window with the URL <https://am.iis.u-tokyo.ac.jp/sso/XUI/#login?realm=/usr&forward=true&spEntityID=https%3A%2F%2Fvpn1.iis.u-tokyo.ac.jp/>. The page header includes the logo of the Institute of Industrial Science, The University of Tokyo. The main heading is “認証アプリによる二要素認証 (TOTP) / 2FA with Authenticator (TOTP)”. Below the heading is a single input field labeled “コード/Code”. A blue button labeled “検証/Verify” is positioned below the field. At the bottom of the page, there is a small disclaimer: “This service includes GeoLite2 data created by MaxMind, available from https://www.maxmind.com”.

On the screen asking if you want to skip the next 2FA, select “No”.

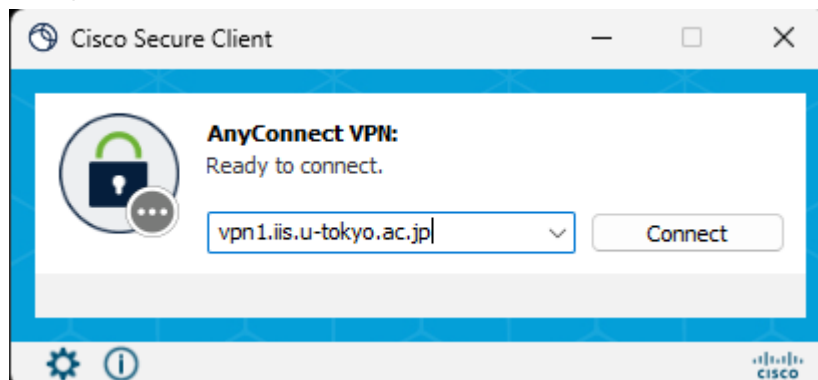


You will be taken to the AnyConnect download screen. Click "Download for ..." to download and install.



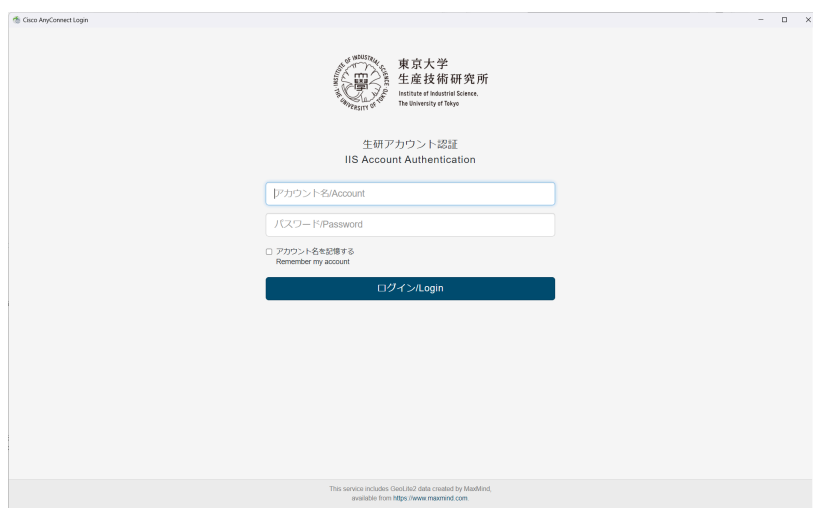
Use of VPN

Start AnyConnect and enter "vpn1.iis.u-tokyo.ac.jp". Click "Connect".
The following instructions are for the Windows version.

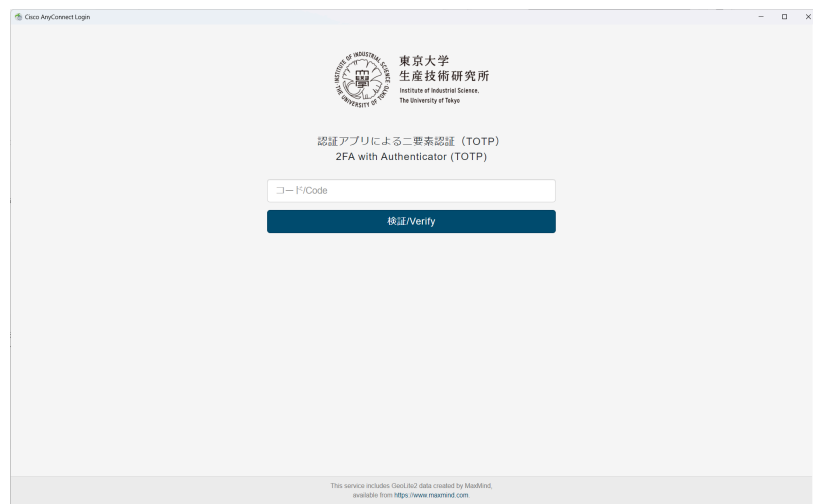


AnyConnect's built-in browser will start and the "IIS Account Authentication" screen will appear. Please enter your IIS account and password.

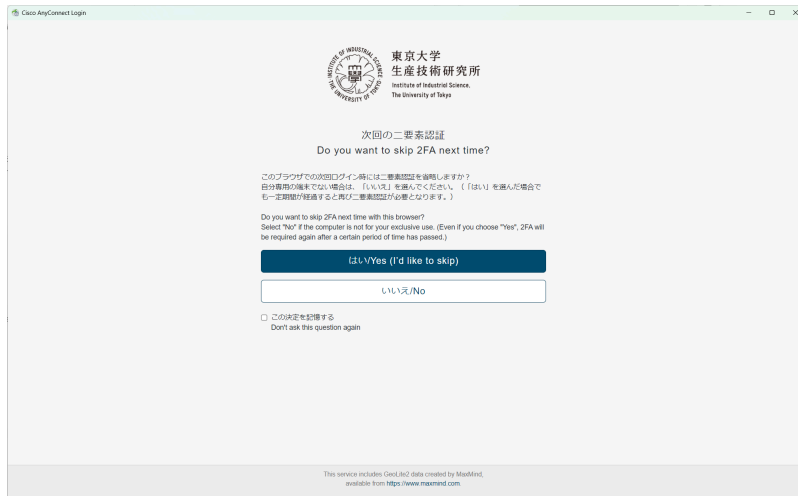
Do not include "@iis.u-tokyo.ac.jp" in the account name because it fails.



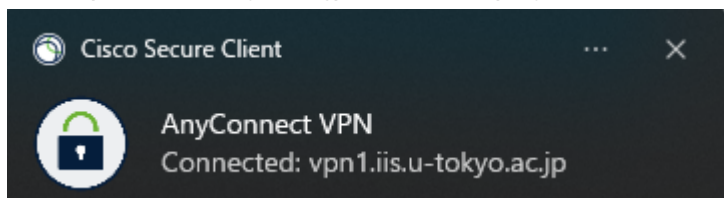
You will be taken to the "2FA with Authenticator (TOTP)" screen. Enter the code displayed on the Authenticator of your smartphone and select "Verify".



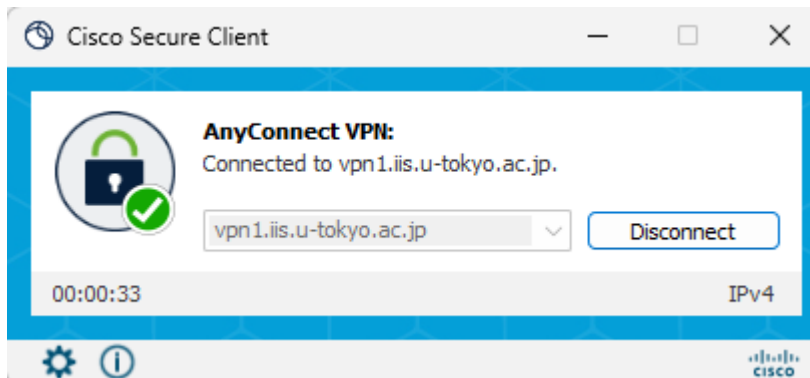
You will be taken to the screen to ask if you want to skip the next 2FA. If you select "Yes" on this screen, you will not need to enter the two-factor authentication code for 30 days when accessing the VPN from the same terminal. If the terminal is not your own, be sure to select "No".



"Connected: vpn1.iis.u-tokyo.ac.jp" will be displayed and the VPN connection will start.



To terminate the VPN connection, click the AnyConnect icon and click "Disconnect".



How to reconfigure two-factor authentication

If you want to reconfigure two-factor authentication due to a change of model or loss of your smartphone, please follow the steps below.

Please log in to the two-factor authentication server:

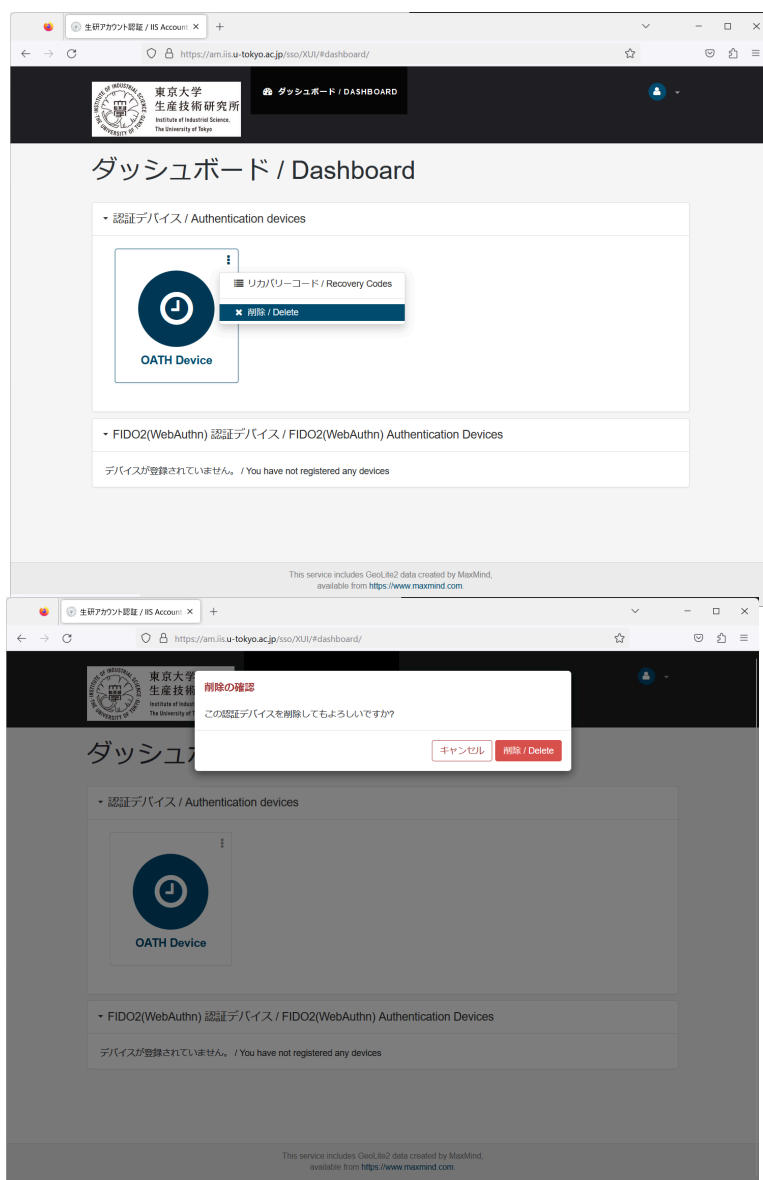
<https://am.iis.u-tokyo.ac.jp/sso/>

If you are in the omission period of two-factor authentication, you do not need to enter the two-factor authentication code.

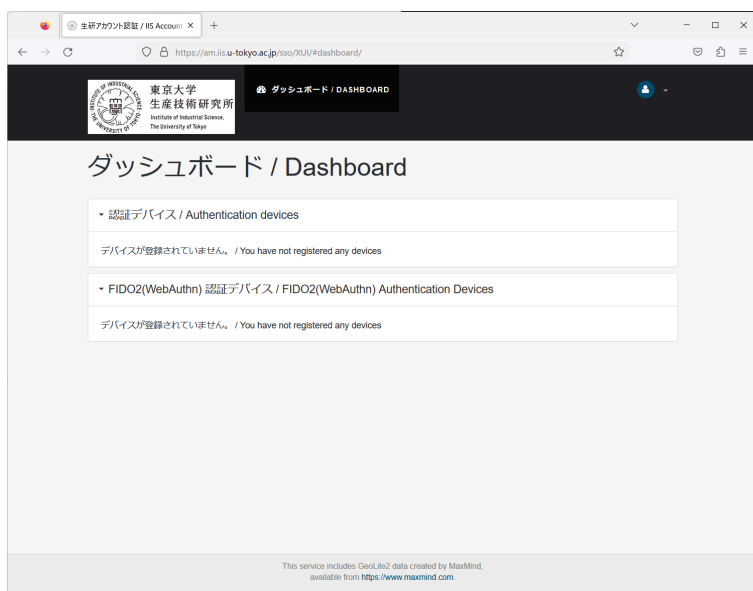
Or use the recovery code for two-factor authentication.

If you cannot log in using the methods above, please email IIS Computer Center at cc-staff@iis.u-tokyo.ac.jp. The subject line of the email should be "(Application) Initialization of two-factor authentication for VPN," and include your affiliation and IIS account.

After logging in, select "Delete" from the ⋮ (three vertical dots) in the upper right corner of "OATH Device".



The item of "Authentication devices" will be in the state "You have not registered any devices."



After logging out, return to the login page. After that, follow the steps in "[Initial setup of two-factor authentication for VPN](#)".

