



**INTERSTATE COMMISSION FOR  
ADULT OFFENDER SUPERVISION**

Ensuring Public Safety for the 21st Century

# ICAOS Website Two-Factor Authentication

## Step 1:

Commission members will log in to the ICAOS website utilizing their current credentials.

The screenshot shows the ICAOS Member Portal. On the left, there is a dark blue sidebar with the text "Member Portal" and a list of resources: "Secure access to ICAOS resources, state data, committee materials, and compliance tools.", "State compact office resources", "Committee documents & meeting minutes", "Commission governance & rules", and "Fee schedules & compliance data". On the right, there is a white login form titled "Sign in" with a "Log in" button and a "Reset your password" button. The form has two input fields: "Username or email address\*" with the value "commissioner" and "Password\*" with masked characters. A "Log in" button is at the bottom of the form.

## Step 2:

You will receive notice that you are required to set up two-factor authentication. Click on the “set up application” link under TFA application.

If your state does not allow an authenticator app per state policy, you can set up authentication through your email by enabling Email OTP.

The screenshot shows the "Validation plugins" section of the ICAOS website. It has three sub-sections: "Recovery Codes" with a "Generate codes" link; "TFA application" with a "Validation Plugin: TFA TOTP" and a "Set up application" link; and "Email OTP" with a "Validation Plugin: TFA Email OTP" and an "Enable Email OTP" link.

## Step 3:

Re-enter your password for the ICAOS website.

The screenshot shows a password confirmation form. It has a label "Current password\*" above a text input field. Below the field is the text "Enter your current password to continue." and two buttons: "Confirm" and "Cancel".

## Step 5:

Select one of the authenticator apps for download on your desktop or mobile device. Once installed, you may be prompted to scan the included QR code in the authenticator app.


Install authentication code application on your mobile or desktop device:

- [Google Authenticator \(Android\)](#)
- [Google Authenticator \(iOS\)](#)
- [Microsoft Authenticator \(Android/iOS\)](#)
- [Twilio Authy \(Android/iOS\)](#)
- [FreeOTP \(Android/iOS\)](#)
- [GAuth Authenticator \(Desktop\)](#)

The two-factor authentication application will be used during this setup and for generating codes during regular authentication. If the application supports it, scan the QR code below to get the setup code otherwise you can manually enter the text code.

3XBMBAYZPQUM640

Enter this code into your two-factor authentication app or scan the QR code below.



Application verification code \*

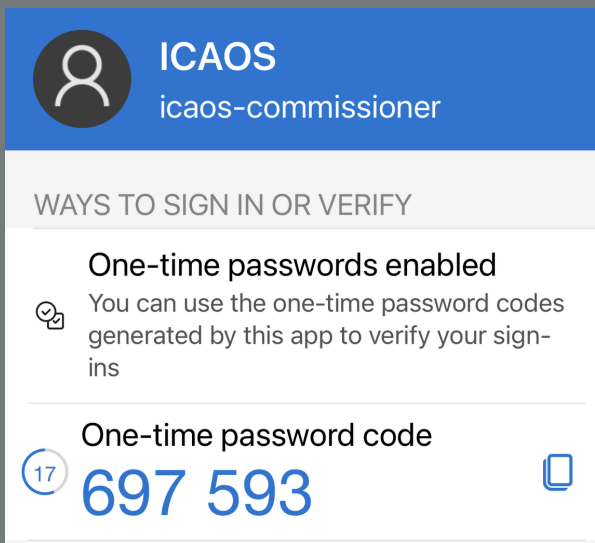
A verification code will be generated after you scan the above QR code or manually enter the setup code. The verification code is six digits long.

[Verify and save](#) [Cancel](#)

## Step 6:

Once set up in the authenticator app, it will generate an application verification code for you to enter on the ICAOS website.

Example shown is the Microsoft Authenticator app.



ICAOS  
icaos-commissioner

WAYS TO SIGN IN OR VERIFY

One-time passwords enabled  
You can use the one-time password codes generated by this app to verify your sign-ins

One-time password code  
17 **697 593**

## Step 7:

To enable email authentication, check the box to authorize the code be sent to your email and click save.

Receive authentication one-time code by email \*

Enables TFA one-time code be sent by email associated to your account email.

[Save](#) [Cancel](#)

Two-factor authentication is essential for protecting sensitive data and meeting CJIS security requirements. It adds an extra layer of protection to ensure only authorized users can access system information.

If you need assistance in setting up your two-factor authentication, please contact the National Office for support.