

Yale University PPMS Core Facility Management System

User Setup Guide for Stratobox-Enabled Instruments

Code-Based Authentication

Access to Stratobox-interlocked instruments requires **Code-Based Authentication**, which links login credentials to reservations for accurate billing.

1. First-Time Setup (In PPMS)

- When attempting to book a reservation from a Stratobox-enabled instrument for the first time, PPMS will prompt you to configure Code-Based Authentication.

The image consists of two side-by-side screenshots from the PPMS website, connected by a large blue arrow pointing from left to right. The left screenshot shows the 'PPMS for the Joe's Demo Core - JDC' website. The top navigation bar has 'Book' highlighted in blue. Below the navigation bar, there's a section titled 'Step 1. Go to Book Systems available for booking'. Underneath, there are several instrument categories: 'Alias', 'Assisted Ali', 'Home Computer', and 'Mid-tier an'. Under 'Home Computer', there is a list of instruments, including 'Stratobox Test (Home)'. A blue arrow points from the 'Book' button in the navigation bar to the 'Stratobox Test (Home)' instrument. The right screenshot shows the 'Configure code based authentication' page. It has a title 'Configure code based authentication:' and a section 'Instructions' with three numbered steps. Below the instructions is a QR code. Under the QR code, there's a section 'Configuration' with a heading 'QR code to scan with your phone.' and a list of options for login: 'Use 2-step authentication for login (password or single sign on + code)', 'Single sign (password or single sign on)', and 'Submit an code provided with the application:'. There is a text input field containing '008710' and a 'Complete configuration' button.

If you have already booked an instrument and have not previously configured MFA, OR if you need to reset an existing MFA configuration:

- In PPMS, go to the header menu and select **Profile**.
- Scroll down and click on **Setup or configure code-based authentication and 2-factor login**.
- Under Set-up a new code authentication configuration, click on **Reset**

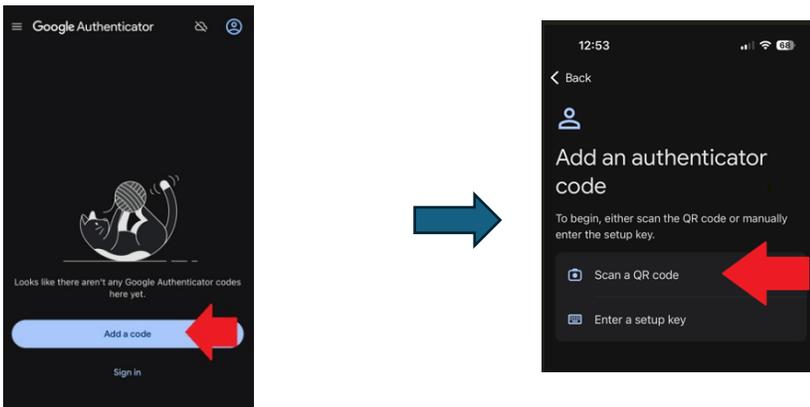
2. Download an MFA App (On Your Phone)

Install a supported multi-factor authentication (MFA) app:

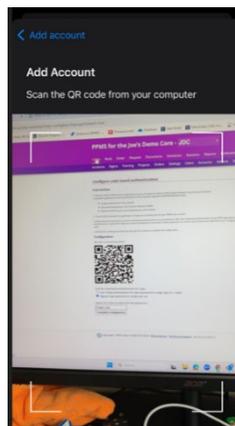
- **Google Authenticator** (recommended, most compatible with PPMS)
 - **Microsoft Authenticator**
 - **DUO Mobile**
-

3. Set Up MFA (On Your Phone)

- Open your chosen MFA app.
- Tap **Add a code**, then next screen **Scan a QR code**.

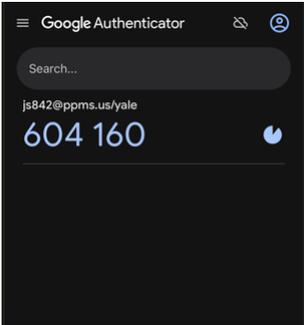


- Use your phone to **scan the QR code** displayed in PPMS.



- Follow the prompts to complete the setup.
-

4. Enable Two-Step Authentication (In PPMS)



Configure code based authentication:

Instructions

1. Please install an Authenticator application on your smartphone (those do NOT require network connectivity to function). Compatible applications with Time-based One-Time Password algorithm (TOTP/RFC6238) include:
 - Google Authenticator: iOS, Android
 - Microsoft Authenticator: iOS, Android, Windows Mobile
 - RedHat FreeOTP open source Authenticator: iOS, Android
2. Scan the QR code with the application to setup your authenticator for your PPMS user account.
3. Select whenever you want to use the code based authentication as a second factor. Note: the code-base authentication setup (TOTP algorithm) is used be mandatory for instrument tracker purposes. As a result, some instruments will enforce the configuration of this code-based authentication mode even
4. Fill the the a code generated by the app and click submit to complete the configuration.

Configuration

QR code to scan with your phone



Use the code-based authentication for login:

Use 2-Step authentication for login (password or single sign on + code)

Regular login (password or single sign on)

Submit an code provided with the application:

355971

User files

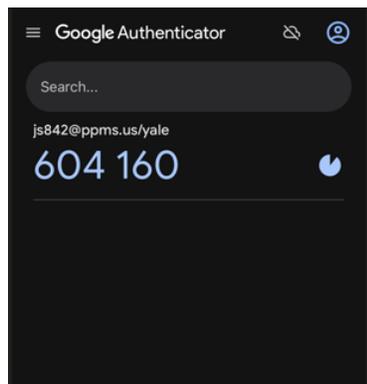
No files

- Return to the Configure code based authentication page in PPMS.
- Select **Regular login (password or single sign on)**.
- Enter the current 6-digit TOTP from your MFA app.
- Click **Complete Configuration**. You are now ready to begin using the MFA to login to the Stratoboxes

Using Stratobox at the Time of Reservation

1. Generate Your TOTP Code (On Your Phone)

- Open your MFA app (e.g., Google Authenticator).
- Retrieve the 6-digit authentication code.



2. Log In to the Stratobox (At the Instrument)

- Enter the TOTP code on the Stratobox keypad, followed by #.



- If the code is correct:
 - Your **username** appears on the display.
 - The **instrument powers ON**.

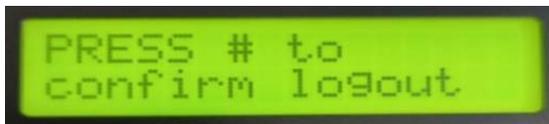


- If incorrect:
 - An **error message** is displayed.



3. Log Out (At the Instrument)

- Press *, then confirm with #.



- If no user is logged in, pressing * refreshes the screen.

4. Automatic Logout

- If power usage drops below **20W for 2 minutes**, a **warning** is displayed.



If no interaction occurs after **1 additional minute**, you are **automatically logged out**.

- Press # to extend your session.

Relay Activation Timing

- **Scheduled Reservations:** The relay activates at the **start time** of your booking.
 - **Walk-Up Access** (if allowed):
 - Ensure a default **COA (charging account)** is assigned in your **PPMS profile** to avoid billing issues.
-