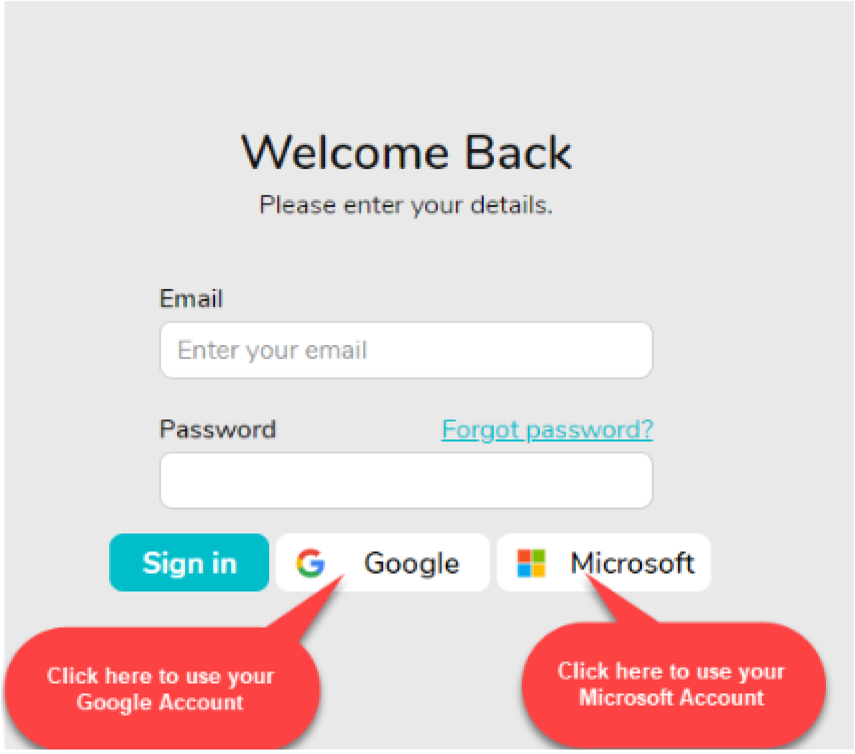
# Single Sign On (SSO) with FYDO

At FYDO, we are committed to continuously enhancing the security and convenience of our platform for our valued customers. And because of that, we use Single Sign On (SSO) to FYDO! This feature will allow you to access FYDO using your existing credentials from Microsoft or Google, simplifying your login process while maintaining the highest level of security.

SSO is a secure authentication process that enables you to log in to multiple applications with a single set of credentials. By integrating SSO, we aim to provide you with a seamless and efficient log in experience.

When you log in, you will notice two buttons for Microsoft and Google account access, as pictured below.



Welcome Back

Please enter your details.

Email

Enter your email

Password

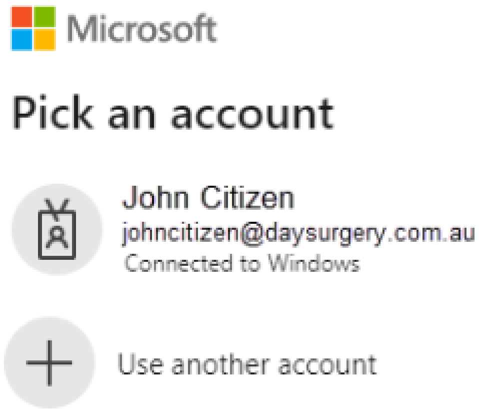
Forgot password?

Sign in
Google
Microsoft
Click here to use your Google Account
Click here to use your Microsoft Account

If you are already logged into your browser with either a Google or Microsoft account, you can click on the applicable button to log in. This will take you directly to the FYDO dashboard or the Two-Step Verification Process via SMS, email, or an Authentication App as usual.

**Note**– The account you use must already be set up in FYDO to proceed.

If you are not already logged into your browser with an account, you will be prompted to **'Pick an account'** or **'Use another account'** as shown below. You will need to enter your password to proceed.

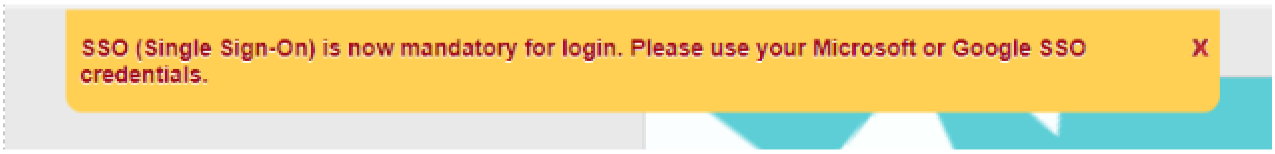

Microsoft

Pick an account

John Citizen
johncitizen@daysurgery.com.au
Connected to Windows

Use another account

You may still use your email and password to log in unless your FYDO account subscriber has forced SSO to be used. In that case, you may receive a message at the top of the screen, as shown:


SSO (Single Sign-On) is now mandatory for login. Please use your Microsoft or Google SSO credentials.

If you receive the message above, please try using the Microsoft or Google buttons. If you still have problems logging in, **contact your FYDO account subscriber** *(the person in charge of FYDO at your facility)* before reaching out to Altura Health Support.

**If you have forgotten your Microsoft or Google password, please contact your IT department. This issue is separate from FYDO and cannot be addressed by Altura Health Support.**

## How to enforce SSO in FYDO

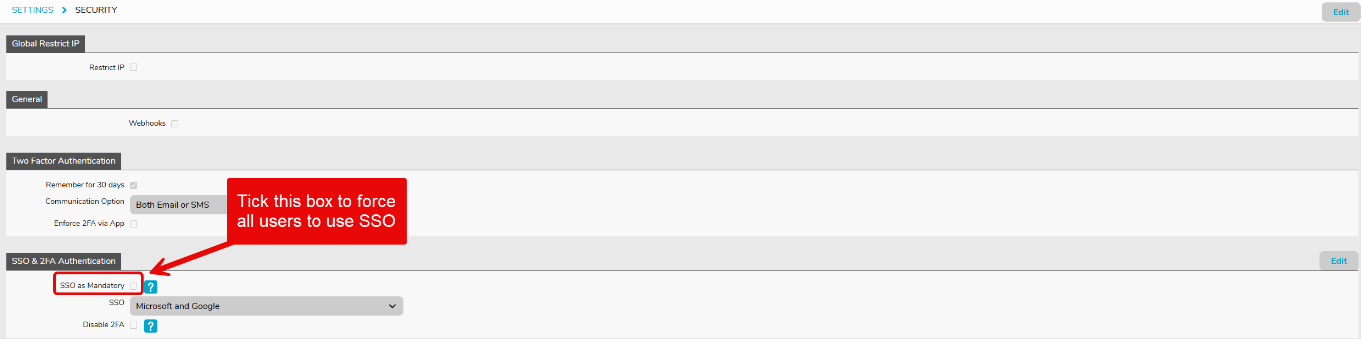
SSO authentication can be enforced for all or selected users. Once SSO is enforced, an email invitation will be sent to the applicable user/s, advising them to activate their account via SSO. The user does not need to use the email invitation link; they can go directly to the FYDO website.

**Note:** Once a user is required to use SSO by their facility, their existing password will be deleted.

To enforce SSO for all users:

1. Go to **Settings > Security** and click **Edit**.

2. Tick the **SSO as Mandatory** tick box (as shown below) and click **Save**.



SETTINGS > SECURITY

Global Restrict IP

Restrict IP □

General

Webhooks □

Two Factor Authentication

Remember for 30 days ☑

Communication Option: Both Email or SMS

Enforce 2FA via App □

SSO & 2FA Authentication

SSO as Mandatory □ ?

SSO: Microsoft and Google

Disable 2FA □ ?

Tick this box to force all users to use SSO

If, for any reason, some users are unable to authenticate using SSO, they can be reverted back to the standard email/password authentication method.

**To revert all users to email/password authentication:**

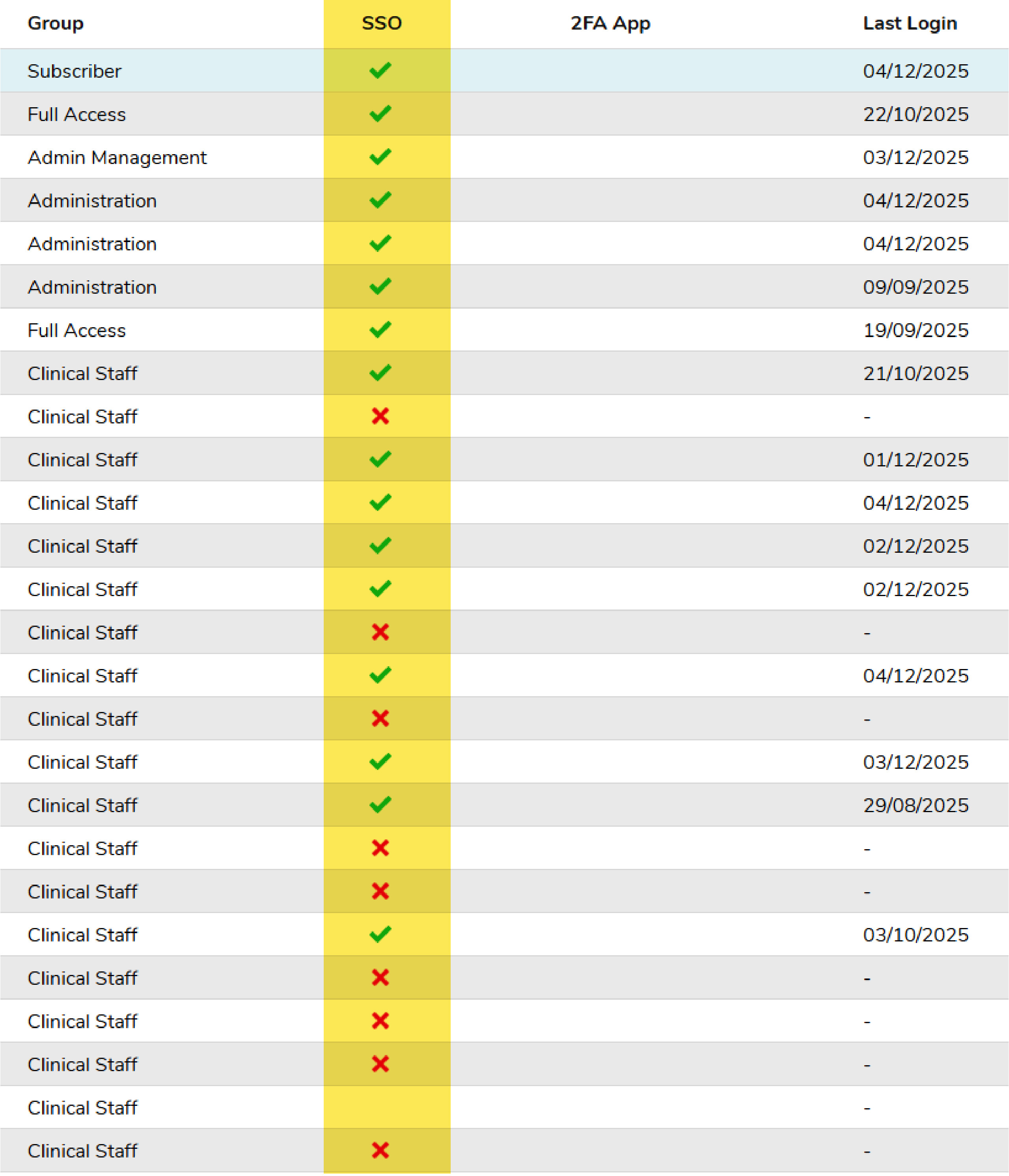
1. Simply untick the **SSO as Mandatory** box in **Settings > Security.**

**To revert specific users to email/password authentication:**

1. Go to **Settings > Users**
2. Double-click on required user
3. Click **Edit**
4. Untick **SSO Mandatory**
5. Click **Save**

Reverted users will receive another email invitation to set up their new password.

You can see which users have SSO enforced and whether they have successfully authenticated using SSO by going to **Settings > Users**.



| Group | SSO | 2FA App | Last Login |
|---|---|---|---|
| Subscriber | ✓ | | 04/12/2025 |
| Full Access | ✓ | | 22/10/2025 |
| Admin Management | ✓ | | 03/12/2025 |
| Administration | ✓ | | 04/12/2025 |
| Administration | ✓ | | 04/12/2025 |
| Administration | ✓ | | 09/09/2025 |
| Full Access | ✓ | | 19/09/2025 |
| Clinical Staff | ✓ | | 21/10/2025 |
| Clinical Staff | ✗ | | - |
| Clinical Staff | ✓ | | 01/12/2025 |
| Clinical Staff | ✓ | | 04/12/2025 |
| Clinical Staff | ✓ | | 02/12/2025 |
| Clinical Staff | ✓ | | 02/12/2025 |
| Clinical Staff | ✗ | | - |
| Clinical Staff | ✓ | | 04/12/2025 |
| Clinical Staff | ✗ | | - |
| Clinical Staff | ✓ | | 03/12/2025 |
| Clinical Staff | ✓ | | 29/08/2025 |
| Clinical Staff | ✗ | | - |
| Clinical Staff | ✗ | | - |
| Clinical Staff | ✓ | | 03/10/2025 |
| Clinical Staff | ✗ | | - |
| Clinical Staff | ✗ | | - |
| Clinical Staff | ✗ | | - |
| Clinical Staff | | | - |
| Clinical Staff | ✗ | | - |

- **SSO Blank:** User not forced to use SSO
- **SSO Red Cross:** User forced to use SSO but not activated
- **SSO Green Tick:** User has activated SSO

# FYDO Security

Rest easy, knowing your FYDO data is protected with layered security controls designed for healthcare environments.

### Secure Infrastructure

- Hosted on AWS in Australia, leveraging robust cloud security and reliability controls.
- High availability options are supported for increased redundancy.
- Backup and restoration strategies are in place to minimise downtime and data loss.

### Data Protection

- Data is encrypted in transit and at rest.
- Encryption applies to stored data and backups.
- Data handling is governed by documented policies and access controls.

### Identity and access management

- Supports Single Sign-On (SSO).
- Multi-Factor Authentication (MFA) is enforced for account access.
- Role-based access controls (RBAC) support least privilege access, users only receive the access they need for their role.
- Administrative access is tightly controlled and monitored.

### Security Operations, Monitoring and Auditability

- Continuous monitoring and protective controls are used to detect and respond to suspicious activity.
- Web application protection controls help defend against common online threats.
- Centralised logging and alerting support traceability and operational oversight.
- Audit trails support investigation and accountability for key system events.

### Secure Development and Change Control

- Secure-by-design practices are applied throughout the software lifecycle.
- Changes are managed through controlled processes to reduce risk and support service stability.
- Vulnerability management practices are in place to identify and remediate security issues.

### Independent Testing and Assurance

- FYDO undergoes regular independent security testing (e.g. penetration testing and security assessments) by third-party security specialists.
- Further security documentation and evidence can be provided during procurement or due diligence, subject to confidentiality arrangements.

### Incident Management

- We maintain incident response processes to manage security events, including investigation, containment, and follow-up improvements.

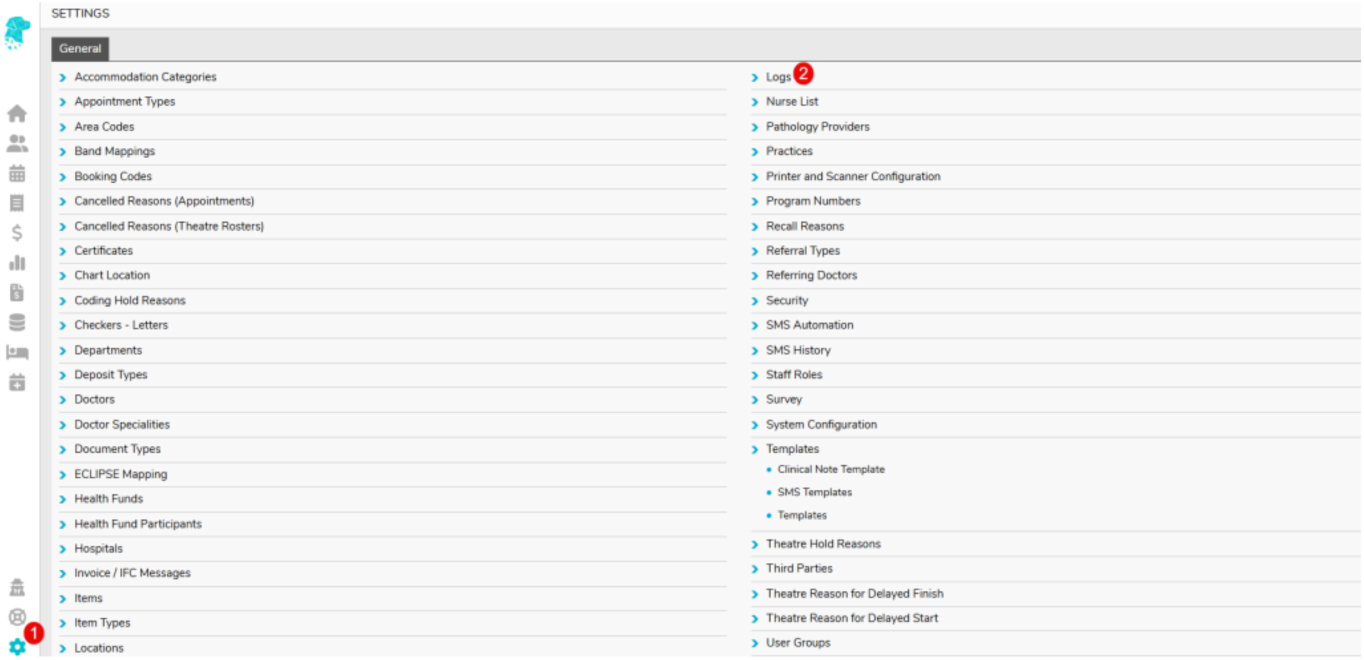
---

# Tracking User Activity in FYDO

Did you know you can view user activity history in FYDO? Whether it’s to track changes made to an invoice, to see when a patient record was deleted or which user undertook what action, and when, the FYDO’s **Audit Logs** feature can help! Read on to learn more.

The audit logs show information about *the action* performed, *who* performed it, *when* they performed it, and their *IP address*. It can be used for troubleshooting purposes or monitoring user activities.

To view the audit logs, first navigate to **Settings**, then **Logs**.

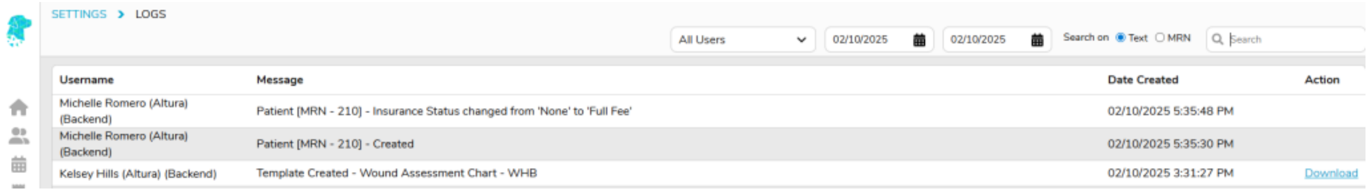


### How is user activity recorded?

Every user login is unique. So when a user logs in and begins taking actions on FYDO, their activity is logged. Here are some examples of logged user activity in FYDO:

- User login
- Changes to patient record
- Changes to appointment details
- Billing and invoicing changes
- Claims sent and batches receipted
- Payments taken, split, or reallocated
- Documents deleted
- Batches removed

You can view user action history within a date range, sort by user, action, or date, as well as search.



All Users 02/10/2025 02/10/2025 Search on ● Text ○ MRN Search

| Username | Message | Date Created | Action |
|---|---|---|---|
| Michelle Romero (Altura) (Backend) | Patient [MRN - 210] - Insurance Status changed from 'None' to 'Full Fee' | 02/10/2025 5:35:48 PM | |
| Michelle Romero (Altura) (Backend) | Patient [MRN - 210] - Created | 02/10/2025 5:35:30 PM | |
| Kelsey Hills (Altura) (Backend) | Template Created - Wound Assessment Chart - WHB | 02/10/2025 3:31:27 PM | Download |

### Why use FYDO’s Audit Logs?

Let’s take a closer look at the benefits of this feature.

1. **Greater accountability**: logged user action history fosters a culture of responsibility by users being aware that their actions are being logged, promoting responsible behaviour within the organisation.
2. **Enhanced troubleshooting**: logged user action history can aid in pinpointing the source and cause of an issue, helping users to troubleshoot problems faster.
3. **Improved security**: logged user action history offers a log of most system activities, enabling the identification of unauthorised access attempts, powering administrators to take the necessary steps to secure the system.

---

# FYDO Two-Step Authentication

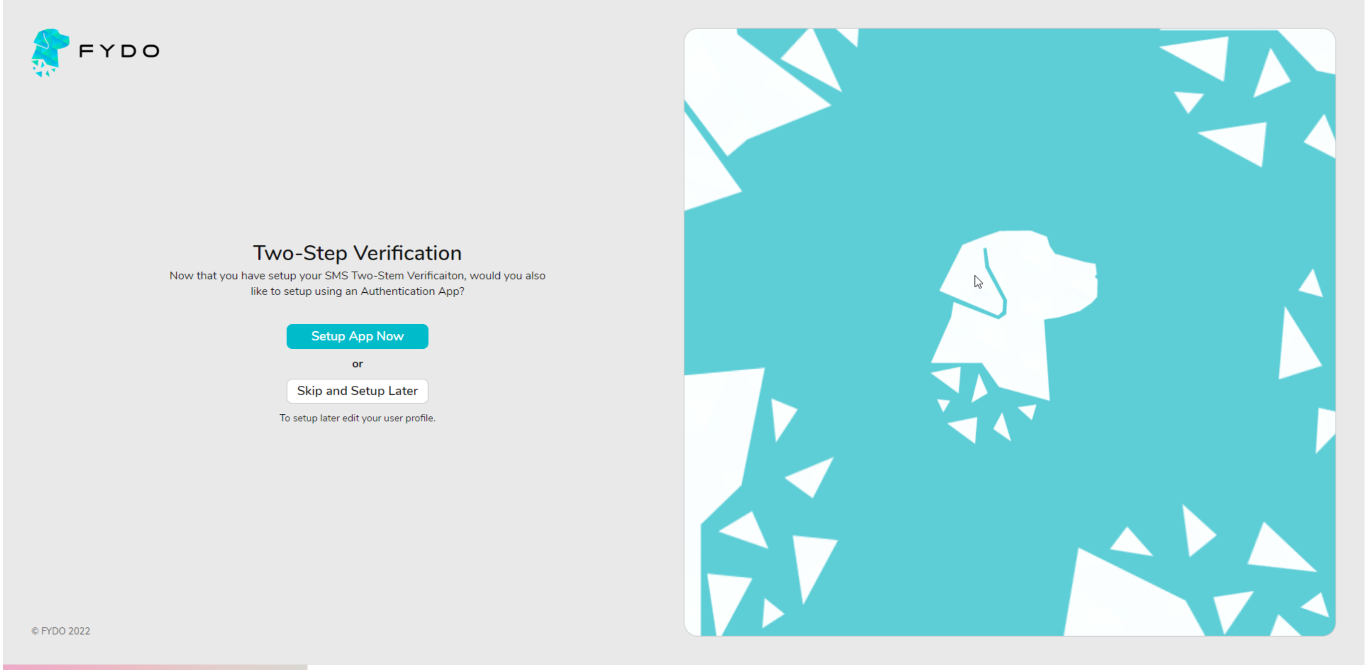
FYDO manages highly sensitive information, which is why Two-Step Verification is mandatory for all users.

Each facility can choose whether users must complete the Two-Step Verification process on every log in, or if they will allow users to choose the option to **Remember me for 30 days.**

Using an Authenticator App *(like Google Authenticator)* is the most efficient and reliable way to complete your **Two-Step Verification**. It’s faster and more dependable than receiving codes by SMS or email, especially in areas with poor reception or slow internet.

You may choose SMS & Email authentication if needed. Just note that delivery can be delayed in low-connectivity areas.

During first log in – You’ll be prompted to **Setup App Now.**

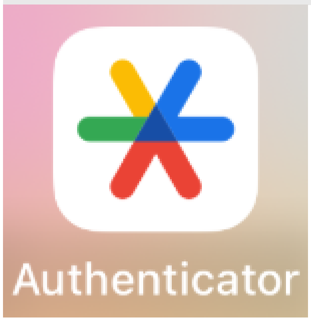


Two-Step Verification

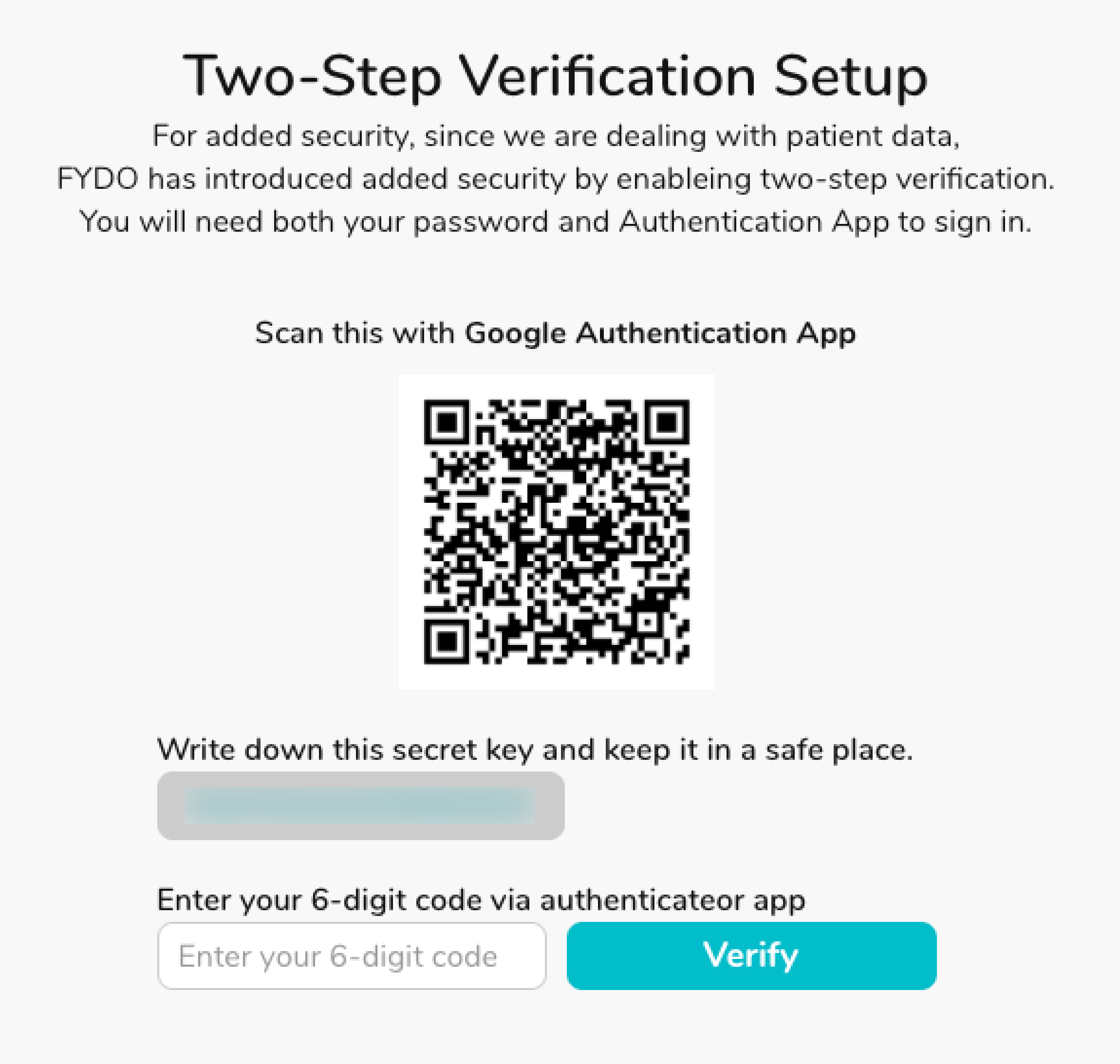
Now that you have setup your SMS Two-Stem Verificaiton, would you also like to setup using an Authentication App?

To setup later edit your user profile.

© FYDO 2022



Download and open the **Google Authenticator App** on your mobile device.
Once the user clicks **Setup App Now,** on FYDO, they will be shown a QR Code that they can utilise the app to scan.



## Two-Step Verification Setup

For added security, since we are dealing with patient data,
FYDO has introduced added security by enableing two-step verification.
You will need both your password and Authentication App to sign in.

Scan this with Google Authentication App

Write down this secret key and keep it in a safe place.

[redacted]

Enter your 6-digit code via authenticateor app

Open the Google Authenticator App & click **Add a Code**. Then select **Scan a QR Code**.

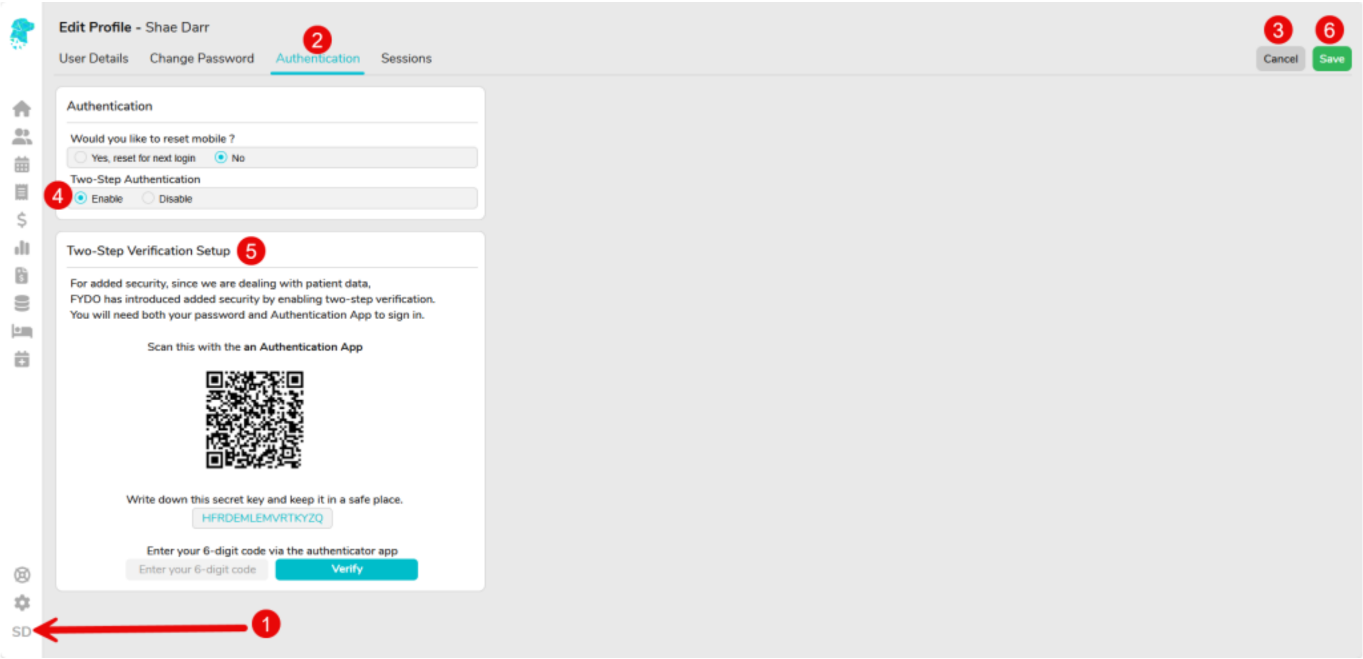
After following the prompts on the app, the user will be able to obtain their 6-digit code to enter into the field before clicking **Verify.**
*(Writing down the secret key & keeping it in a safe place will allow users to access their account in the case that they misplace their mobile phone)*

Want to set up later? Just click **Skip and Setup Later.** You can continue with SMS or Email verification and set up the app when you're ready.

[redacted]

To enable app-based verification later:

1. Go to your **User Profile** and click **Edit Profile**
2. Open the **Authentication** tab
3. Click **Edit**
4. Tick the **Two-Step Authentication > Enable** box
5. Follow the instructions on the page
6. Click **Save**



Edit Profile - Shae Darr

Authentication

Would you like to reset mobile ?

○ Yes, reset for next login ● No

Two-Step Authentication

● Enable ○ Disable

Two-Step Verification Setup

For added security, since we are dealing with patient data,
FYDO has introduced added security by enabling two-step verification.
You will need both your password and Authentication App to sign in.

Scan this with the an Authentication App

Write down this secret key and keep it in a safe place.

HFRDEMLEMVRTKYZQ

Enter your 6-digit code via the authenticator app

Enter your 6-digit code

If the facility allows users to utilise the **Remember me for 30 days** option, then the authentication process will only need to be performed once a month. However, if this function isn't allowed by the facility, then this authentication process will need to be met each log in.

---

# Altura Health Data Storage & Security Policy

This policy explains, at a high level, how Altura Health safeguards information to prevent loss, unauthorised access, or misuse. It also outlines our approach to backups and restoration.

## Data Storage and Residency

- Customer data is hosted in Australia using AWS.
- Data is encrypted in transit and at rest using industry-standard encryption.
- Access to systems and customer data is controlled using least privilege principles and role-based access.

## Data Governance and Handling

- Data access is restricted to authorised personnel and governed by documented processes.
- Logging and auditability controls support traceability and accountability.
- Data retention and deletion are managed in line with contractual and regulatory obligations.

## Backups and Restoration

- Backups are performed regularly using cloud-native services.
- Backups frequency and retention vary depending on the product, environment, and data type (e.g. databases vs documents).
- Backup storage is protected using access controls and safeguards to reduce the risk of unauthorised access, deletion or modification.
- Restoration procedures are documented and maintained. Recovery time depends on the nature of the incident and the impacted component.

## Monitoring and Assurance

- Operational monitoring is used to support backup integrity and availability.
- Periodic backup checks and restore testing are performed to validate recoverability.

## Security Assurance

- Altura Health undertakes regular independent security testing (e.g. penetration testing and security assessments) with third-party specialists.
- A summary of recent security assessment results may be provided on request, subject to appropriate confidentiality arrangements.

## Account Access

- Altura Health Supports Single Sign-On (SSO) where configured and enforces Multi-Factor Authentication (MFA) for account access.
- Altura Health supports RBAC, and each facility decides the role structure and is responsible for assigning and maintaining user access for their team.
- Authentication and access controls may vary depending on customer configuration and agreed requirements.