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.

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.

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:

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

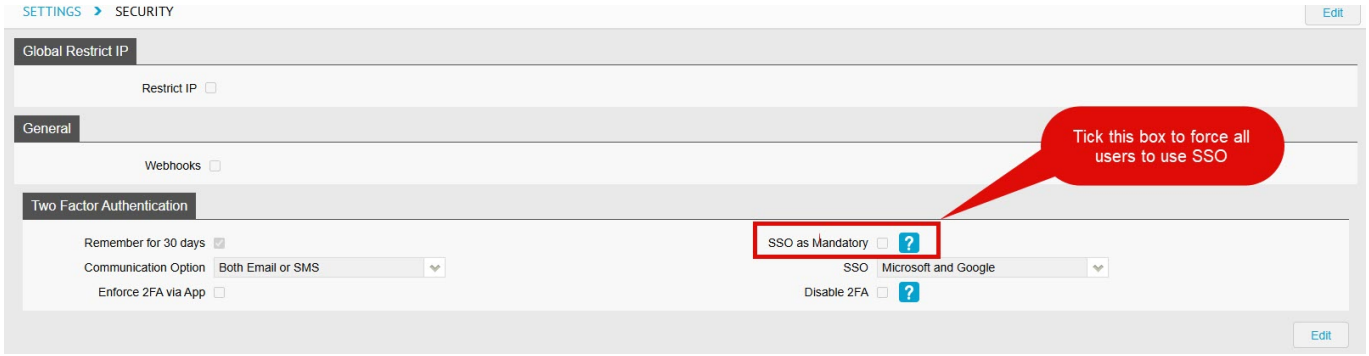
SSO authentication can be enforced for all or selected users. Once SSO is enforced, an email invitation will be sent to the applicable user/s, advising them to activate their account via SSO. The user does not need to use the email invitation link; they can go directly to the FYDO website.

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**.



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**.

- **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 well protected with the following features:

Secure Infrastructure:

- *Data Hosted with AWS in Australia:* Your information is stored in one of the world's most secure cloud environments, ensuring reliability and compliance.
- Options for High Availability data servers for increased redundancy.
- Backup and restoration strategies in place to minimise downtime and data loss.

Advanced Threat Protection:

- *Intrusion Prevention and Detection Systems:* We actively monitor for any suspicious activities and take immediate action to keep your data safe.

Web Application Firewall:

- *Defend Against Online Threats:* Our powerful firewall shields your web applications, providing an additional layer of protection.

End-to-End Encryption:

- *Data Encrypted in Transit and at Rest:* Your sensitive information is safeguarded from start to finish, both during transmission and while stored.

Identity and Access Management:

- *IAM using SSO with MFA:* Securely control who has access, with Single Sign-On and Multi-Factor Authentication for an added layer of identity protection.

Access Control:

- *Geo-blocking and IP Restricted Access:* Control access based on location and specific IP addresses, ensuring only authorized users can connect.
- Provide staff with only the access they need.

Regular Audits:

- FYDO undertakes regular penetration tests from multiple leaders in the Cyber Security industry.

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.

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.

Who can view the Audit Logs?

Any user can be given access to view the audit logs by the Subscriber for their facility. The access is granted or removed in **Settings** > User and **User Groups**.

FYDO Two-Step Authentication

FYDO deals with sensitive information, which is why we have made Two-Step Verification mandatory for all users.

Each facility is able to decide if they want users to have to meet the Two-Step Verification requirements on every log in, or if they will allow users to choose the option to **Remember me for 30 days.**

The most efficient & easy way to meet these requirements is to use the **Two-Step Verification App**. It allows for increased security & will save time for users as it is a more reliable & timely option than receiving the verification code via SMS or Email.

SMS & Email are also available options, however these are not recommended for areas of poor mobile reception or slow internet speed as this can delay their delivery time.

When users log in, they will be prompted to **Setup App Now.** Users will need to download the **Google Authenticator App** to their mobile phone. Once the user clicks **Setup App Now** they will be shown a QR Code.

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)

Users are also given the option to **Skip and Setup Later,** when they first log in, and proceed with using the SMS or Email option for Two Step Authentication. Users will be able to go back and set the App up, when it is convenient for them, by:

1. Going into their **User Profile**
2. Selecting the **2 Step Authentication** tab
3. Click **Edit**
4. Tick the **Allow Google Authentication** box
5. Follow the instructions on the page
6. Click **Save**

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

The purpose of this policy is to explain how Altura Health safeguards all information to prevent loss or misuse of data.
It outlines the important timeframes regarding backups & the information restoration processes that apply to all Altura Health customers.

Database

- All data is stored on Amazon servers located within the SYD data centre
- All data is encrypted at rest and in transit

Backups

- The database is backed up every 6 hours
- The documents e.g. imported document & typed letters are backed up once daily
- Backup restoration can be performed within 24 hours
- Backups are stored on Amazon storage servers

Security

- Altura Health engages in regular penetration testing and certification with third party industry experts
- A copy of the most recent security assessment results can be obtained by contacting us via email at support@alturahealth.com.au or by calling 02) 9632 0026

Account Access

- FYDO requires 2 step authentication which can be setup either via email, SMS code or google authenticator
- Each account is given the option to do this each login, or utilise the 'Remember me for 30 days' feature