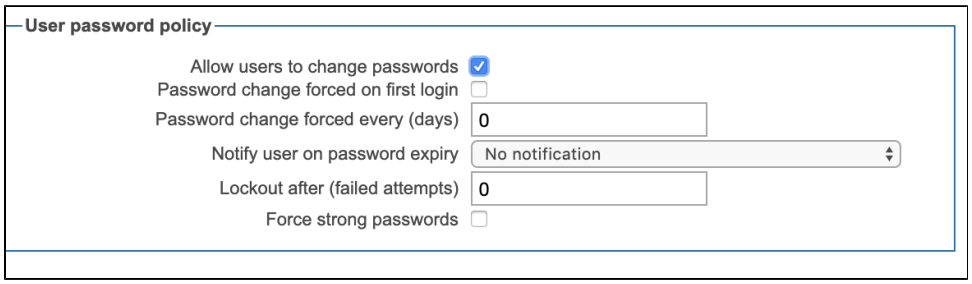
Identity & Access Management

1	Does the solution support Single Sign-On integration?	Yes, Maytech support Single Sign-On and ADFS integrations. Maytech's customers can sign in to their accounts using their existing corporate Active Directory credentials or any other identity provider (i.e. Duo, Okta, OneLogin, etc.).
2	Does the solution distinguish user roles and admin roles within the application?	FTP-Stream: All users except admin are jailed to their home folders and cannot see files or folders outside. To exchange confidential files with customers give each login a distinct home folder. Account owners can add new secondary admins who can help to manage FTP-Stream account and Billing admin, who helps with payments and invoices. In Quatrix there are several user roles that determine what actions can be performed in the account. The account owner is the top administrator of the account that has access to all Quatrix features and can purchase more users for the account. Admin has the same rights as the account owner with the exception of tracking and paying invoices for the account. Pro users can browse folders and share to any of your users or to their contacts who don't need a licence to download (normally your employees). Associate users can only use your service to share files back to your Pro Users - great for external partners who need to regularly feed data into your organisation. Jailed users are jailed to the Projects Shared With Me folder. They are not able to use the Share Form or otherwise share files outside of the designated workflow. Read more about Roles and permissions.
3	How are user passwords stored in the system?	Passwords are individually salted and stored in a database, encrypted one way.
4	Does your organisation have a documented password policy? If YES, describe the controls (e.g. minimum length, complexity, expiration period).	Yes. ISMS OP 30 - Password Management Policy: The following are general recommendations for creating a Strong Password. A Strong Password should: • Be at least 8 characters in length • Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z) • Have at least one numeric character (e.g. 0-9) • Have at least one special character (e.g. ~!@#$%^&*()_-+=) A Strong Password should not: • Spell a word or series of words that can be found in a standard dictionary • Spell a word with a number added to the beginning and the end • Be based on any personal information such as user id, family name, pet, birthday, etc. With the optional Extended Authentication module, customers can set a password policy, including: Users can / cannot change their passwords, must change their passwords on the first login, must periodically change their passwords, must use strong passwords.

<table>
<tr>
<td>5</td>
<td>Can we request a custom password policy to be applied to Customer users?</td>
<td>Yes, the administrator of FTP-Stream account can set a password policy for his/her account to specify complexity requirements and rotation periods for his users' passwords. It provides a possibility to allow users change their passwords, to set a number of failed login attempts, to set the minimum password length, to force password change on the first login or after a specified period and to specify password construction requirements.

The following options are available for configuring the password policy:

Quatrix supports strong passwords.</td>
</tr>
<tr>
<td>6</td>
<td>What is the password reset process?</td>
<td>There are several ways of changing the password in FTP-Stream and Quatrix:

<table>
<tr><th>Admin</th><th>User</th><th>Backoffice Admin</th></tr>
<tr><td>resets his own password;

sends password reset links to his users</td><td>changes his own password.</td><td>resets password upon customer's request.</td></tr>
</table>

The user or admin can change their password on the Login page. Follow these steps:

1. Go to the Login page of your account and click the Forgot password link.
2. Enter your email to get instructions on how to reset your password.
3. Click the Password reset button in the email.

• Password reset link is valid for 24 hours after the first request. All further requests use the same link.
• After 24 hours the link is invalidated and a user has to generate a new link.

1. The Reset password page opens where you should type in and confirm your new password.
2. You can log in to your account with the new password.</td>
</tr>
<tr>
<td>7</td>
<td>Does the solution support multi-factor authentication?</td>
<td>Yes, all Maytech's file sharing products offer Two-Factor Authentication (2FA) as an additional module.

Administrators can elect to have their 2FA codes sent in one of two ways:

1. Download and install the Google Authenticator, Duo Mobile, Authy, or Windows Phone Authenticator app for your phone or tablet. An installed app implements TOTP security tokens from RFC 6238 in a mobile app. It provides a 6 digit one-time password which users must enter alongside their user name and password every time they log in to their account.
2. SMS
During account login an SMS is sent to the user's designated phone number with a one-time use code which is 6 digits long. This code must be entered as well as the user name and password during login.</td>
</tr>
<tr>
<td>8</td>
<td>Do Maytech provide audit and monitoring of access to the system and data?</td>
<td>Yes. Comprehensive audits logs are available and all user activity is tracked.</td>
</tr>
</table>

9	How does the solution authenticate users to prevent unauthorized access?	Username and strong password, and 2FA.
10	Within the application, and the supporting infrastructure, describe how administrator actions are logged and recorded, including details of how long these audit logs are stored for.	Where Maytech are instructed to access any data (regardless of whether it is personal data or otherwise), all such access is logged with information identifying the Maytech's personnel accessing the data and setting out the date and time of access. Access logs are maintained for 12 months and can be downloaded and stored by the Customer at that time.
11	What is your review processes, manual or automated, for event and application logs generated within the solution?	Maytech's approach to log management is controlled by ISMS OP 22 - Logging and Audit Trails Policy. Maytech conduct an ongoing collection and retention of a record of user activities on or with Maytech, including: • Log-in attempts. • Password changes. • File creations, changes and/or deletions. All audit entries are time-stamped with entries recorded as GMT dates and times. Clock synchronisation is uniform on all servers to ensure timestamps are consistent across all logs to avoid any time discrepancies which may cause issues for any subsequent forensic activities. All logs are reviewed periodically (minimum at least monthly) to identify any unauthorized access to the systems. Retention of audit files is for at least 12 months.
12	If required, what methods and formats are available for a Customer to export a copy of data?	The account owner has access to all the data, so can take a copy of it at any time.