Studio 3T

Protecting your Team Sharing data

Security measures

At 3T, we take security very seriously and we've made sure Team Sharing is secure at all times and compliant with data regulations.

Infrastructure and Storage

Studio 3T uses a virtual infrastructure with application servers hosted by Amazon Web Services (AWS) and a MongoDB Atlas database.

The MongoDB Atlas managed service provides:

- A configuration in its own Virtual Private Cloud (VPC)
- Security updates that are automatically applied by MongoDB
- Encryption of data at rest by the MongoDB Encrypted Storage Engine
- Monitoring of status and alerts in case of anomalies

Team Sharing Security Measures

Before data is sent to MongoDB, it is encrypted using MongoDB's Client-Side Field Level Encryption. The data in transit is protected by HTTPS and is encrypted using TLS. API endpoints require an access token.

The following security measures have also been implemented:

- Each shared folder has its own data key. The master key is stored in the AWS Key Management Service.
- Shared data is stored with the email address of the user that shared the data, and includes any user actions that resulted in an error.
- Anti-spam measures limit the number of invitations that can be fetched at a time from the API and the number of pending invitations for a single user.
- Team Sharing uses Redis as a caching layer which is protected in a VPC.
- 3T employs accredited independent professionals to carry out comprehensive penetration tests on a regular schedule.

Users and Access Management

Team Sharing can be turned off to prevent any sharing of data other than the Studio 3T licensing and telemetry data.

The following security measures have also been implemented:

- Before using Team Sharing, users must verify their email address. Single Sign-on users are considered as verified. Users must re-verify their email address, if privileges have been revoked.
- Administrators of user licenses can block access to Team Sharing for all email addresses that are associated with a license.
- Viewing the content of a folder is restricted to users who are folder members.
- Folder access can be revoked or modified at any time by folder administrators with Manage access.
- When sharing connections, users cannot share passwords or certificates. However, passwords are stored locally on the user's computer when a connection is shared, so that each user can have their own username and password for that connection.

Privacy

3T Software Labs is based in the EU and adheres to German privacy laws, GDPR, and UK GDPR.

See our Privacy Policy.

Contact our Sales team if you have any additional questions about security and Team Sharing at sales@studio3t.com