



Content decryption and sensitive records

What content decryption means for messaging records, why it is not offered on this website, and how to work with our support team on sensitive information.

Future service. Wise Network does not provide a content decryption application, download or online decryption service. Nothing on this page is compatible with another provider's decryption tool.

Online version: <https://wisenetwork.co/support/decrypt-content/> · Content updated 28 October 2026

What content decryption means

Some messaging platforms store message text encrypted, or show it masked in reports, so that staff and customers cannot read sensitive content such as passcodes or personal data by default. Decryption is the controlled process of revealing that text when there is a legitimate reason, for example a dispute or a legal request.

Well-designed decryption processes share some features:

- **Separate roles.** The person who requests access is not the person who approves it.
- **Split or protected keys.** No single person holds everything needed to decrypt; keys are kept in a key management system or hardware security module.
- **Strong sign-in.** Access requires multi-factor authentication.
- **Narrow scope.** Only the specific records needed are decrypted, for a limited time.
- **Audit trail.** Every request, approval and decryption is logged and reviewed.

Availability at Wise Network

There is no decryption application, download or online service on this website, and there is no Wise Network customer portal that stores encrypted message content. If you hold an encrypted file from another provider, use that provider's own tools and procedures.

Sharing sensitive records with support

When a support case needs message records, logs or reports that contain personal data:

1. **Ask first.** Email support@wisenetwork.co describing the case without attaching the sensitive data.

2. **Share the minimum.** Send only the fields needed, for example message IDs, times and masked numbers, rather than full content.
3. **Use an agreed secure transfer.** We will agree a method with you; do not send passwords, keys or full message text by ordinary email.
4. **Agree retention.** Agree how long the data is kept and confirm deletion when the case closes.

See our [privacy policy](#) for how we handle personal data.

What a future decryption service would need

If Wise Network introduces stored, encrypted message content, a decryption feature would require at least: a defined list of the data stored and why, managed encryption keys, approved roles and approval steps, multi-factor sign-in, audit logging, a legal basis and retention rules for each market, and independent security testing. It would be documented on this page before launch.

Questions? Email support@wisenetwork.co. This PDF is generated from the web page above; the online version is the reference.