



Encryption

Encryption in Zoho Assist

Encryption is primarily used to safeguard the contents of a message so that only the intended recipient can read it. This is achieved by replacing the contents with unrecognizable data, which can only be unscrambled by the intended recipient. This protects the data from anyone who might want to steal it.

There are two ways to use encryption:

- Encryption in Transit
- Encryption at Rest (EAR)

Encryption in Transit

Encryption in transit refers to data that is encrypted when it is in transit, including from your browser to the web server and other third parties via integrations. Encrypting data in transit protects your data from man-in-the-middle attacks.

[Learn more about Encryption in Transit.](#)

Encryption at Rest

Encryption at rest refers to data that is encrypted when it is stored (not moving), either on a disc, in a database, or some other form of media. Encrypting data when it is stored on the servers provides an even higher level of security than just using encryption in transit. EAR protects against any possible data leak due to server compromise or unauthorized access.

How data is Encrypted in Zoho Assist?

Encryption is performed at the application layer using the *AES-256* algorithm which is a symmetric encryption algorithm and uses 128-bit blocks and 256-bit keys. The key used to convert the data from plain text to cipher text is called the Data Encryption Key (DEK). The DEK is further encrypted using the Key Encryption Key (KEK), providing yet another layer of security. The keys are generated and maintained by our in-house Key Management Service (KMS).

[Learn more about our KMS.](#)

What data is encrypted in Zoho Assist?

Our servers encrypt and store the screenshots and session recordings captured during Zoho Assist remote support sessions and unattended access sessions.

Full-disk encryption

In addition to application layer encryption, full disk encryption is available in the India (IN), Australia (AU), and Japan (JP) data centers.

[Learn more about full-disk encryption.](#)