Client Data Protection FAQs

Where does Entrust host client data?

Entrust distributes client data between multiple cloud services, namely Amazon AWS, Microsoft Azure, and Microsoft Office 365. Each platform meets the highest standards for enterprise-tier data protection and routinely passes physical and IT security audits.

How does Entrust protect unauthorized access to client data?

Entrust employees must regularly update their corporate passwords with complexity requirements suggested by modern security standards. We also require all employees to maintain multi-factor authentication for their Entrust accounts.

What steps does Entrust take to limit employee access to client data?

Entrust utilizes multiple real-time monitoring procedures to supervise and control employee access to internal systems and client data.

We grant employee access to client data on a need-to-know basis. If an employee does not require client data to fulfill their duties, they are not granted access.

How does Entrust monitor IT security and compliance?

Every year, Entrust undergoes a third-party IT security and compliance audit. The independent auditor reviews our vendors, service providers, policies, and procedures to ensure that our IT security practices meet appropriate standards.

How does Entrust protect clients from identity theft and account fraud?

Entrust utilizes LexisNexis for identity verification and fraud prevention. This solution guards against account impersonation and protects client accounts from unauthorized use by malicious parties.

Additionally, all client data is encrypted at rest and in transit using ciphers and encryption. This practice mirrors the approach of IT security standard-bearers such as Google, Amazon AWS, and Red Hat. We regularly review and adjust our data protection methods to match upgraded security and resilience protocols.

How does Entrust protect client data in the Entrust Client Portal?

The Entrust Client Portal provides clients with several multi-factor authentication options. We only allow encrypted access to the portal, requiring clients' browsers to support and accept a secure connection to our servers. Otherwise, access will be denied.

Further, we do not store or retain client passwords in plain text or decryptable form. Nor are we able to restore a plain text password once it has been accepted by the system and saved in the database.