

Security



SmartSimple handles client data with the utmost integrity. Security features and functionality exist at all levels of our system, from administrative controls to encrypted servers which are securely housed in a SSAE 16 (SAS 70*) data center.

Certifications, Memberships & Compliance

SSAE 16 (US), CSAE 3416 (Canada), FS-ISAC (Financial Services - Information Sharing and Analysis Center)

Encryption & Protection

- SHA 256 Password Encryption • SSL (128/1024) Encryption • Closed ports • All outward-facing URLs are encrypted
- Encrypted servers (provides protection from “bare metal attacks”) • DDoS Shield

Role-Based Permissions

The creation of user roles that define levels of access is central to the SmartSimple platform. This user level control ensures that information is only accessible to those who are authorized.

System Lockdown

At the first sign of an attempted breach of security, your version of SmartSimple can be placed on lockdown. This ensures that access is limited to parties who are addressing the security concern.

Forensic Auditing

With your permission, SmartSimple can track system usage and provide you with detailed access reports. This may help to identify any unauthorized access resulting from issues such as shared passwords and malicious data manipulation.

Reader Log and Field Change Tracking

All field changes are tracked and auditable.

Two-Factor Authentication

Protect your organization and system by requiring an additional layer of user verification beyond a username and password. Two-factor authentication drastically reduces the incidence of online identity theft and fraud.

Upgrades



SmartSimple currently updates and upgrades the system on a bi-monthly basis. These upgrades are backwards compatible, enhance the system and do not require action from users.

*SSAE 16 supersedes Statement on Auditing Standards (SAS) No. 70 with the professional guidance for performing a service auditor's examination.