Transcription workflow software in the cloud

www.ScribeManager.com

ScribeManager Security

NB: The provisions in this document are subject to change without notice.

In BRIEF:

ScribeManager is a cloud-based transcription workflow system that incorporates the following security applications:

- Hardware firewall as a first line of defence against malicious traffic. The firewall contains its own OS and operates independently of its server. Offers packet inspection, port blocking, and more.
- HTTPS secure web interface. 256-bit ssl (secure socket layer) to encrypt online transactions and prevent phishing attacks
- ScribeManager's server is housed in a secure US location with limited access, motion-detecting cameras, and earthquake-proof walls.
- Encrypted password system - only you know your unencrypted password
- Password-protected downloads - files can be downloaded only by users who are logged in

- Files encrypted during upload and on server (maximum file size may apply)

In DETAIL:

Features	Description
Data protection during file transfer	
File transfer	ScribeManager employs SSL/TLS protocols to protect client authentication, authorization and file transfers.
High-grade encryption	ScribeManager secures files in transit with no less than 128-bit encryption using industry-standard encryption protocols.
File integrity	ScribeManager employs a keyed hashed message authentication code (HMAC) to authenticate and ensure the integrity of intra-system communications. ScribeManager verifies file size and file hash to ensure integrity.
Link generation	ScribeManager download links are uniquely and randomly generated using strong hash-based message authentication codes. ScribeManager provides technical countermeasures to protect links from guessing attacks.
Data protection during storage	
Datacenters	ScribeManager uses SSAE 16 Type II accredited or ISO 27001 certified datacenters to host the SaaS application and metadata. All files are stored in SSAE 16 Type II (SOC1), SOC2 and ISO 27001 accredited datacenters with high availability and durability ratings.
Encryption	ScribeManager stores client files at rest using AES 256-bit encryption, a Federal Information Processing Standards (FIPS) encryption algorithm.
Firewalls	Files are processed using systems protected by securely configured firewalls that effectively limit and control access to network segments.
Redundant storage	Files are stored in replicate with leading Infrastructure-as-a-Service (IaaS) providers that ensure high file durability and availability.
Backup	Files are backed up according to configurable file-retention and versioning settings.

The best way to see how ScribeManager can help you is to try it free for a month. To do that, visit the "try it free" page on this site. There's no set-up fee and no credit card is required. To ask questions first, please contact our friendly support via the the scribemanager website: http://www.scribemanager.com.

Configurable settings	
Password policy	Clients have the option of configuring password policies, including password history, expiration, and complexity controls such as length, uppercase and lowercase letters, at least one number, and at least one special character
Custom SMTP (mail) settings	ScribeManager enables clients to route email messages though their own mail servers. When enabled, all emails sent through ScribeManager will be routed through the client's mail server, instead of ScribeManager mail servers. Clients may optionally configure the connection to support SSL.
Multi-factor authentication	Clients may set up a multi-factor (or strong) authentication process that requires submission of the account password and a secondary authentication, such as Google Authenticator or SMS/text message, in order to access the account. ScribeManager supports various two-factor and two-step authentication methods including forms and token-based authentication as well as SMS, voice and backup codes.
File retention	Users can choose to automatically delete files a certain number of days after upload to support retention preferences and policies.
Terms and conditions	Terms and conditions can be displayed on the login page, with the option of including a check box on the login screen that must be marked to indicate compliance with the terms before logging in.
FTP/FTPS	By default, file transfers occur over HTTPS (Port 443). Optionally, clients can connect to ScribeManager using FTP or FTP over SSL (FTPS connection over port 990), an inherently more secure protocol than FTP. Users can connect to ScribeManager directly from an FTP/FTPS program, providing a way for users to upload or download files to or from a secure location while using existing FTP/FTPS programs.
Account lockout	ScribeManager can configure your account to lock for five minutes after five invalid logon attempts to prevent account tampering. This application control is an account preference that can be customized to meet individual compliance needs.
Email notifications	Users can have customized notifications sent in real time.
Access log retention	Detailed file-access logs are retained for at least one year.

The best way to see how ScribeManager can help you is to try it free for a month. To do that, visit the "try it free" page on this site. There's no set-up fee and no credit card is required. To ask questions first, please contact our friendly support via the the scribemanager website: http://www.scribemanager.com.