convene
Smart. Simple. Secure.

System Security Features

convene
Smart. Simple. Secure.

Overview

Azeus Convene provides excellent user experience in holding meetings, as well as sharing, collaborating and accessing documents—without compromising security. By using Convene, users can securely access documents, organize meetings, and conduct presentations with mobile devices in both online and offline mode.

Convene is designed and developed with an emphasis on responding to the challenges of enterprises and public services that require data protection, control, availability, and application security. Built with strong encryption mechanisms throughout the system, Convene's web portal allows user administrators to centrally manage user accounts, system policies, file access rights, and monitor system user activities.

At a Glance

- SSAE16- and ISO27001-Compliant Cloud Hosting
- 2048-bit SSL
- AES-256 network and document encryption
- Multiple-factor authentication by device registration
- On-the-fly decryption
- Fine-grained access control
- Automatic purge for lost devices
- Audit trail

Infrastructure Security

- Hosting facilities in the US, UK (Ireland), Singapore, and Australia are SSAE16- and ISO 27001-certified.
- Unaffected by Heartbleed Vulnerability (a serious bug found in the open-source OpenSSL cryptography library — CVE-2014-0160).
- Daily automated backups ensure data integrity. Unused or obsolete backups are destroyed and replaced to prevent unauthorized data retrieval.
- Continuous network monitoring of any attempted network attacks. Our staff closely monitor servers in real-time to ensure optimum system performance.
- Convene servers undergo operating system hardening. Login is secured by strict access controls and encrypted access. Administrative access is restricted to authorized personnel only.
- Proxy Server Support

Network & Document Encryption

- Wireless network transmissions between Convene and its web portal are encrypted via 2048-bit Secure Sockets Layer (SSL)
- Network transmissions between Convene devices are encrypted using 256-bit Advanced Encryption Standard[1]
- Documents are always encrypted with AES-256 when stored in Convene's local storage and web portal

Secured Decryption on Mobile Devices

Convene uses a secure, on-the-fly decryption model. When the user needs to access encrypted files on storage, only the needed parts are decrypted into memory. In contrast, common encryption software decrypts the whole document and stores its decrypted form on

[1] communication between devices use an initial 1024-bit RSA connection before upgrading to a 256-bit AES connection to facilitate a secure transfer of the AES key

temporary file storage, which hackers can access. In addition, Convene uses automatically-purged local storage for its temporary files. Files are never backed up to iTunes and iCloud.

Key Management

- Data is protected by three-tier key management with random document key, user key and system key
- In Convene, user keys are securely stored in the iOS Keychain and protected by iOS device-specific encryption with automatic key generation, transfer and destruction
- System Administrators only need to keep and manage the system key to control overall security

User Authentication, Password and Login Session

- Log in to both Convene and its web portal with a single user account
- Strong password policy and password expiration period is enforced
- Allow only your registered devices to sign in to Convene to prevent anyone else from accessing your account with an unregistered device.
- Password is encrypted using AES-256
- Protect meetings through the attendee list
- Automatically sign out users on session timeout

Access Right Control

- Access rights can be granted to an individual user or user group
- Allows automatic access right inheritance from parent to subfolders and files to ensure proper access right control while minimizing administrative effort
- Allows individual password protection for specific files and folders
- Read-only and read-write permissions
- Role-based access permissions to files in the portal and meetings

Security for Lost Devices

- Authentication prevents unauthorized access to data on a lost device
- Multi-level encryption keys and key management reinforce key protection, which is important especially when a device gets lost
- Data on a lost device is automatically purged when password guessing is detected
- When password guessing is detected, the system automatically locks the dubious user account and wipes out offline data/cache.

Audit Trail

- Track all login attempts
- Track all file uploads and downloads
- Track all file permissions granted to users and user groups

Physical Security

24x7 physical security of hosting facilities encompasses all computer and network communication systems.

Information Security

Information security controls are governed by strict internal access policy involving provisioning and change control. All employees are trained on data security requirements.

Security Testing

Application and infrastructure penetration testing are performed regularly.