

Key Features

- Policy enforcement and metadata removal
- Password-protected file and link sharing with permissions and policy-based access per folder
- All transactions authenticated against user accounts
- Flexible permission settings to choose whether members can forward, download, comment on, or access files after a specified date
- Administration controls for access revocation and permission adjustments
- Sophisticated data encryption with RC4-128 Secure Sockets Layer (SSL) encryption in transit and 256-AES encryption at rest
- Network protection and segregation with multiple connectivity and CDN partners
- Privacy and information security policies set to comply with HIPAA, SAS70 Type II, and ISO 27001

Workshare offers a range of desktop, mobile, and tablet applications for secure enterprise collaboration.

Workshare cloud infrastructure delivers enterprise-class data security and availability to safeguard digital content, prevent unauthorized access, and guarantee availability.

Workshare is hosted by a range of carefully selected and fully accredited data center partners across Europe and North America, allowing organizations to locate their data in a region of their choice.

Enhanced Data Security

User authentication

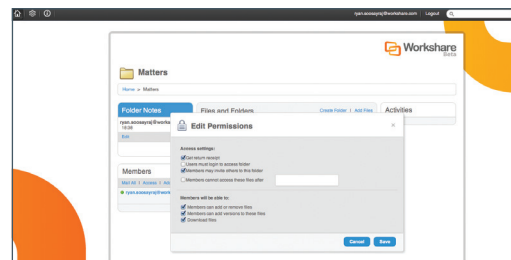
All transactions with Workshare must be executed from within the context of a personal, authenticated user account. Access to view or edit content stored or shared with Workshare is only possible once users have been authenticated by creating unique passwords and verifying their email addresses.

SSL encryption

Workshare encrypts personal information and digital content with RC4-128 Secure Sockets Layer (SSL) technology when the files are in transit and 256 AES encryption at rest to ensure that no one else can read it.

Application-layer security

Workshare stores all files in a proprietary, binary-fragmented format rather than the original format. This means that files are unintelligible except to users and guests who have gained authenticated access through Workshare.



Flexible permissions

Workshare offers flexible permission settings to choose whether members can forward, download, comment on, or access files after a specified date.

Policy Enforcement

Permissions

Authors of a documents can decide, when sending on for collaboration, exactly who can have access.

Metadata removal

Users can create customizable profiles for metadata cleaning, PDF conversion, and URL replacement.

Large file transfer

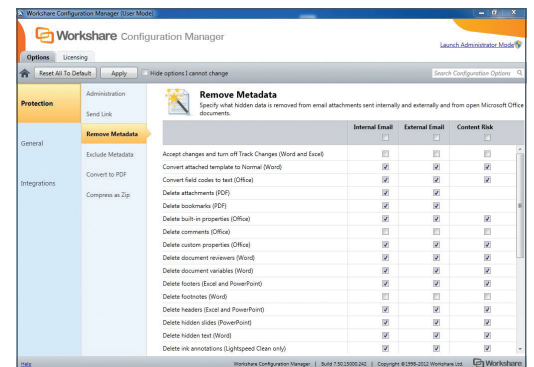
Administrators can set policy ensuring any email attachment of a pre-defined size will be sent as a link.

Expire old links

Specify an expiration date for the file, after which the recipient will no longer be able to access the file.

Password access

Force recipients to have a Workshare Platform user account to access the file.



Secure data and IP

Workshare policy designer reduces the commercial risk posed by inadvertently sharing confidential or sensitive documents by automatically applying compliance rules defined by IT administration or functional leads.

Advanced Data Center Architecture

Data center architecture

Workshare data center partners are ASHRAE, ISO 27001 Information Security Management System (ISMS), and/or SAS70 Type II audited/certified. North American partners are also Federal Information Processing Standard (FIPS) and healthcare-applications compliant with HIPAA's Security and Privacy Rules.

Physical security

Workshare's partners' data center buildings are protected with multiple layers of physical security: a perimeter fence, a security gate and entrance, an alarm system, mantraps, biometric access systems into Workshare's footprint, CCTV, trained security staff on site 24x7, and an external security firm to patrol the area both inside and outside. No one enters or leaves without proof of identity, and all visitors are checked against defined access lists.

Controlled environment

For optimum performance, all equipment is maintained and continuously monitored in a climate-controlled environment (chiller, CRAC, fire panels, generator, UPS, etc.). Multiple CRAC units provide redundant capacity (N+1). Fire-retardant walls, early-warning laser smoke detectors (VESDA), direct lines to fire stations, and automatic, gas-based fire suppression systems provide protection against fire. All the facilities' infrastructures are monitored 24x7.

Power

Workshare partners provide power with a minimum N+1 power infrastructure configuration. This mission critical infrastructure offers the flexibility to scale as required without losing overall efficiency or disrupting the infrastructure's availability.

Network infrastructure security

The core network infrastructure segregates traffic to prevent eavesdropping. Workshare network gateways are hardened against spoofing attacks and employ packet filtering and policy routing. Unused switching device ports are disabled. Workshare maintains independent, source-controlled package repositories and employs upstream package staging to secure binary packages, fast-track security, and bug fixes.

Data access controls

Workshare partners employ a variety of mechanisms and security checks to control data access. All Workshare employees undergo criminal background, credit and social security checks, as well as employment verification. Access to the network infrastructure is limited to facility managers and network engineers. Support staff use individually generated public/private key authentication, which is more secure than traditional passwords.

Contact us

North America:

+1 415 975 3855 / 888 404 4246

Europe:

+44 20 7426 0000 / +49 6227 381 111

Asia:

+61 2 8220 8090 / +852 2251 8985

sales@workshare.com

www.workshare.com/contactus

About Workshare

Workshare is a leading provider of secure enterprise collaboration and communication applications. The Workshare platform allows individuals to easily create, share and manage high-value content anywhere, on any device. Workshare enhances the efficiency of the collaborative process by enabling content owners to accurately track and compare changes from contributors simultaneously. The integrated Workshare platform also reduces the commercial risk posed by inadvertently sharing confidential or sensitive documents. More than 1.8 million professionals in 70 countries use Workshare's award-winning desktop, mobile, tablet, and online applications. For more information visit www.workshare.com or follow Workshare on twitter at www.twitter.com/workshare.