KONICA MINOLTA

KOMI Doc

AUTOMATE BUSINESS PROCESSES

RETHINK SECURITY

Keep your data safe and secure with KOMI Doc

Giving Shape to Ideas

YOUR DATA SECURITY AND PRIVACY ARE OUR PRIORITY

We are committed to maintaining data security at all times. Your data and their security are at the heart of our concerns.

To enable your teams to evolve in a constantly changing world and to respond to their new work habits, we have implemented an advanced, multilayered security program.

Working from home, in the office or on the move requires flexibility, but above all flawless security at all levels to effectively prevent leaks, misuse of information or limit the impact of cyber-attacks.

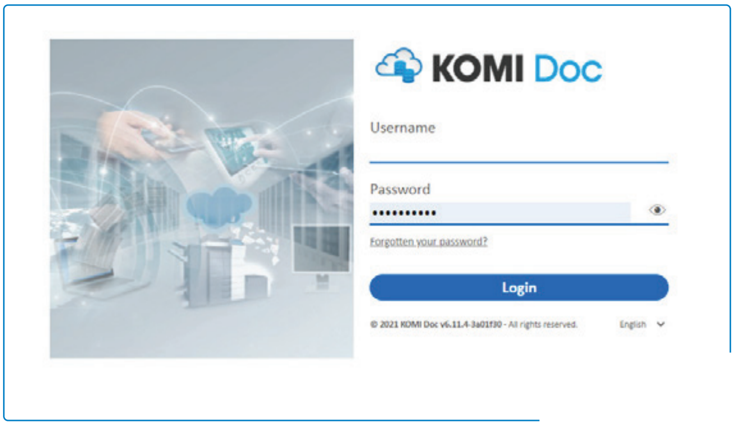
This document details KOMI Doc platform security capabilities, our operational security, data privacy and regulatory compliance measures that ensure the confidentiality, integrity and availability of your data.

APPLICATION SECURITY

STRONG PASSWORD POLICY

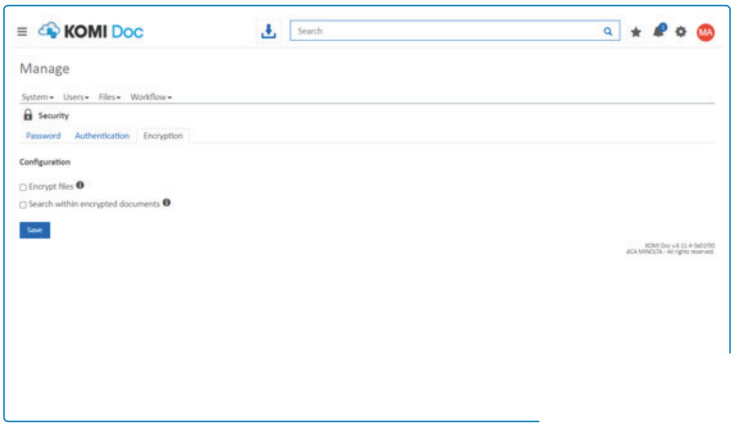
To protect against dictionary-based, brute-force attacks, KOMI Doc integrates advanced features for administrators:

- **Credentials Policy :** Passwords must meet minimum length and complexity criteria. Users are required to regularly change their passwords.
- **Lock-out policy :** user accounts are locked after a configurable amount of failed login attempts, and for a configurable lock out duration
- **Session Time-out :** After a configurable period of inactivity users are required to sign in again.
- **Two Factor Authentication (2FA) :** upon sign-in, users are asked to key-in a five-digit security code (received by email or via Google Authenticator) in addition to their password



© 2021 KOMI Doc v6.11.4-3a01f30 - All rights reserved.

Passwords are transmitted via a hypertext transfer protocol secured (HTTP with TLS) connection



Configuration

□ Encrypt files

□ Search within encrypted documents

KOMI Doc v.6.11.4-3a01f30
KA MINOLTA - All rights reserved.

ENCRYPTION

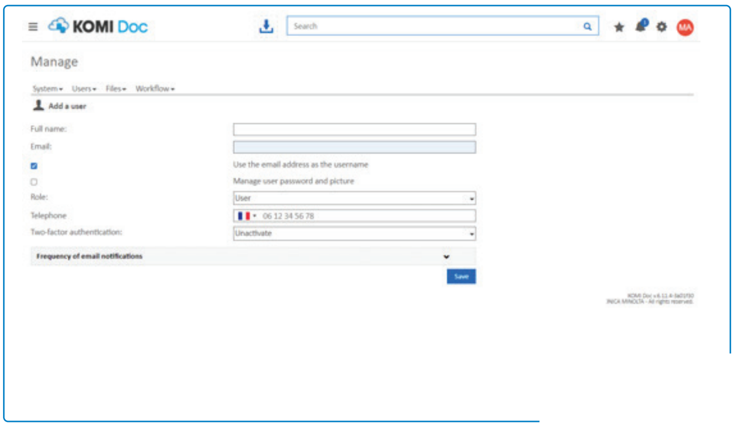
- **Data in transit :** KOMI Doc establishes a secure TLS connection to provide communications security over public computer networks, encrypting all communication between the web server and users browser
- **Document Security 'At-rest' :** All documents stored on KOMI Doc server (either in the cloud service or on-premises appliance) can be encrypted using industry standard 256-bit Advanced Encryption Standard (AES)

APPLICATION SECURITY

ONBOARDING AND USER PROVISIONING

To automate the creation and removal of users accounts, KOMI Doc administrators benefit from multiple secured option:

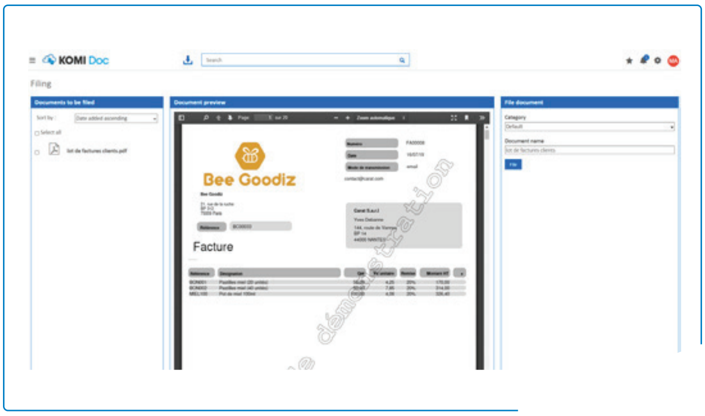
- **Active Directory :** Integrate your existing Active Directory (AD) instance with KOMI Doc to simplify and centralize users & groups management
- **Single sign-on (SSO) :** KOMI Doc platform integrates with many SAML 2.0 compliant services to provide users with a single sign-on (SSO) solution.
- **API :** Rest API support the development of custom user provisioning and identity management solutions



Full name:
Email:
☑ Use the email address as the username
□ Manage user password and picture
Role: User
Telephone: 06 12 34 56 78
Two-factor authentication: Unactivate
Frequency of email notifications

CONTENT SECURITY

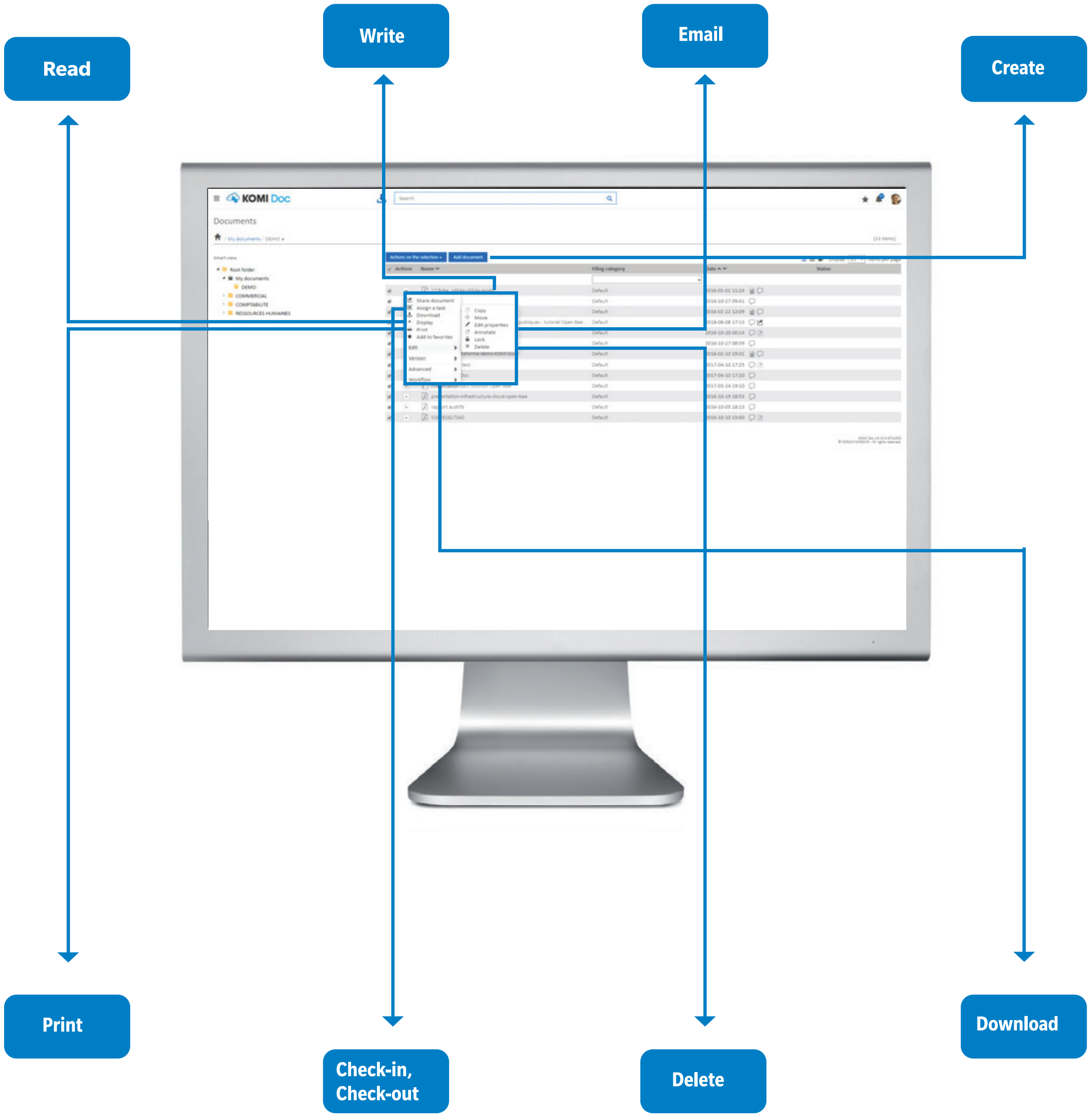
- **Granular content permissions :** Administrators can manage access rights on folders and documents by assigning access right to groups and users (Full Control, Edit, Read, Print, ...)
- **Digital Watermark :** Watermarking disables print and download and add a "stamp" in the form of the user login and date to the original document to dissuade users from engaging in data theft
- **Tracking and Control :** Administrators can view the audit trail; the complete history of any activity being performed on a document inside KOMI Doc.
- **Sharing controls :** Administrators can authorize shared links before documents are communicated to external contacts.



Sort by: Date added ascending
□ Select all
□ lot de factures clients.pdf
Category: Default
Document name: lot de factures clients

FOCUS ON GRANULAR LEVEL PERMISSIONS

In KOMI Doc, the system administrator can manage access rights for users and groups according to the following criteria:



DATA CENTER INFRASTRUCTURE SECURITY

KOMI Doc cloud applications are hosted in Microsoft Azure highly available data centers in the UAE (Dubai) and Asia (Singapore), with a global uptime average of > 99.99 %.

Microsoft Azure

PHYSICAL SECURITY

- Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored.

- Microsoft understands the importance of protecting your data, and is committed to helping secure the datacenters that contain your data. We have an entire division at Microsoft devoted to designing, building, and operating the physical facilities supporting Azure. This team is invested in maintaining state-of-the-art physical security.

- Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources. Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. More info here

COMPLIANCE

Microsoft Azure infrastructures meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. They also meet country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

For a full list of compliance standards that Azure adheres to, see the Compliance offerings

CLOUD MONITORING

All KOMI Doc servers and services are automatically monitored and report any system failures or performance bottlenecks immediately.

AUTOMATED BACKUP

KOMI Doc instances hosted in the Cloud are registered by a policy designed to maintain data integrity and availability to prevent loss of data and to facilitate the restoration of documents and configured business processes.

Data are being backed up on a daily basis with following retention rules (set of policies about how long Data are archived):

- Daily: 14 days

- Weekly: 12 weeks

- Monthly: 24 months

Certified Data Centers that host KOMI Doc are designed to protect information systems from natural, environmental hazards and unauthorized intrusion.

Standards compliance	
Azure compliance (ISO 27001, SOC 1, SOC 2 SOC 3, ...) offerings are based on various types of assurances, including formal certifications, attestations, validations, authorizations, and assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents produced by Microsoft.	For more information please **read**
Security	
Video surveillance	✓
Security company 24 hours a day, 7 days a week	✓
Access control to the rooms	✓
Fire services protection	✓
Redundant power supply	✓
Tier IV-equivalent datacenter	✓
Diesel generators and redundant power inverters	✓
Hosting services	
Installation and configuration of production servers	✓
Infrastructure monitoring (24 hours a day and 7 days a week)	✓
Security management (antivirus, firewall, confidentiality)	✓
Updates, corrective patches and others migrations management	✓
Data backup and recovery	✓
Backup duplication on a remote site	✓
Data securing with AES 256 encryption	✓
Automated mechanisms of load distribution (load balancing)	✓
Possible connection to the company private network with VPN	O
Bandwidth use rate monitoring	✓
CPU and RAM use rate monitoring	✓
Storage space monitoring	✓
Maximum time of incidents notification ensured by SLA	✓
Maximum time of incidents resolution ensured by SLA	✓

✓ = included, O = optional

VULNERABILITY & RISK MANAGEMENT

Our security team carry out regular automated and manual security testing and patch management, and work with third-party specialists to identify and remediate potential security vulnerabilities and bugs.

KOMI Doc applications has successfully passed security penetration tests on :

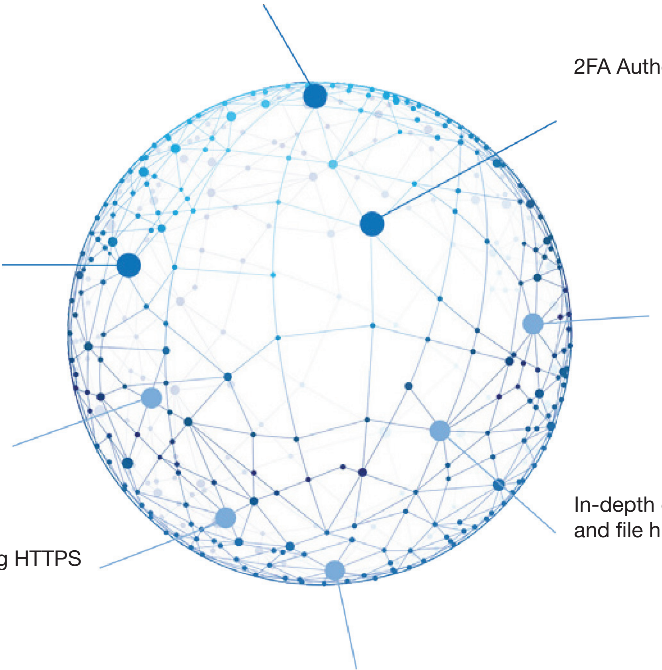
- Solution design and architecture
- Source code analysis and review
- Solution features analysis including User management, Authentication, Authorization, Data confidentiality, Integrity, Accountability, Session management, Transport security, Tiered System Segregation, Privacy
- Manual and Automatic Penetration testing using web application vulnerability scanners, binary analysis tools, proxy tools

KOMI Doc application is frequently tested for common vulnerabilities such as those listed in the OWASP Top 10 :

1. Injection. Injection flaws, such as SQL, NoSQL, OS, and LDAP injection.
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration, Weak session management
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Cookies poisoning
10. Buffer overflows

MAKE SURE YOU ARE PREPARED...

KOMI Doc integrates the most advanced computing security technologies for maximum privacy and security.



External Sharing :
Password protection + Expiration Policy

2FA Authentication

Granular permissions
(from view- and print-only or fully editable,
dynamic watermark...)

Data Segregation: logical isolation to segregate each customer's data from that of others

Files & folders encryption at
Rest with AES-256

In-depth capabilities to log and track user activity and file history, compliance reports

Encryption in Transit using HTTPS

Datas back-up

CONTACT US

Konica Minolta offers a comprehensive range of solutions spanning access control, data security, network security and scanning security, with functionalities varying from one device to another. **Get in touch with us** today to find out how we can tailor the best solution to help you secure your data and corporate environment.