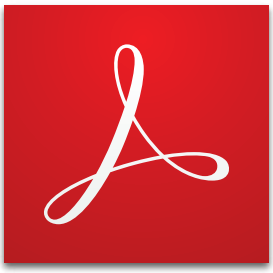
Adobe Document Cloud security



Adobe Document Cloud helps organisations worldwide transform document processes and deliver compelling digital experiences to engage customers, get business done faster and compete more effectively. Seamlessly integrating into your existing enterprise systems and business applications, Document Cloud solutions include Adobe Sign and Acrobat DC, along with mobile and web applications, flexible APIs and turn-key integrations. Document Cloud empowers departments across your organisation to increase operational efficiency, reduce risks associated with human error and create intuitive end-to-end digital experiences.

At Adobe, security practices are deeply ingrained into our internal culture, software development and service operations processes. Whether related to identity management, data confidentiality or document integrity, Document Cloud employs industry standard security practices to help protect your documents, data and personal information. Document Cloud solutions are supported by a comprehensive network of technology, people and strategic partnerships that protect your data with industry-leading security standards that allow your organisation to adapt to changing environments and meet market demand with advanced workflows, easy licence management and robust cloud infrastructure.

Security at its core

Adobe takes the security of your digital experiences seriously. Adobe is constantly monitoring and improving our applications, systems and processes to help customers meet the growing demands and challenges of securing and protecting data. Document Cloud services, including *Adobe Sign* and PDF services, use a rigorous approach to help ensure the confidentiality, integrity and availability of your documents. Today, Document Cloud data centres are maintained in multiple geographically dispersed regions and operated by Adobe trusted partner Amazon Web Services (AWS). Each AWS data centre includes state-of-the-art physical, environmental and access controls as described at *https://aws.amazon.com/security/*.

Additionally, the Adobe Secure Product Lifecycle (SPLC)—a set of specific security activities spanning software development practices, processes and tools—is integrated into multiple stages of the Document Cloud product lifecycle. To protect from the physical layer up, Adobe implements a foundational framework of security processes and controls for our infrastructure, applications and services. For additional information about Adobe security processes, community engagement and the Adobe Secure Product Lifecyle, please see *www.adobe.com/uk/security.html*.

Disaster recovery

Adobe maintains a high level of operational excellence and works to ensure that customers are not impacted by unplanned outages. If there is an unplanned outage, Document Cloud operations personnel work as quickly as possible to restore full access to the service as soon as possible. The data centres are designed to tolerate system or hardware failures with minimal customer impact.

Environmental controls

All Document Cloud data centres are equipped to detect environmental hazards and utilise climate control systems to maintain a consistent operating temperature and humidity level per SOC 2 Type 2 certification requirements.

Data encryption and privacy

Adobe products and services, including Document Cloud, are designed with privacy in mind. Document Cloud encrypts documents and assets at rest using the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) 256-bit encryption and supports Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security (TLS) to ensure that data in transit is also adequately protected.

Document Cloud employees and trusted vendors only access customer data to perform certain business and support functions, or as required by law. Adobe does not provide any government with direct or systematic access to customer data that we store. For more information about Adobe's privacy policies please see *www.adobe.com/uk/privacy.html*.

Intrusion detection and system monitoring

The threat landscape is ever evolving and increasingly challenging, so Document Cloud uses a variety of monitoring systems to detect network security anomalies, denial of service, IP spoofing, port scanning and other advanced cyberattacks. Adobe operations security teams use a set of monitoring alert criteria to define the critical security and availability standards for our services' production environments along with third-party monitoring tools to closely monitor any spikes in activity above pre-hardened thresholds. Adobe security operations teams also deploy Intrusion Detection System (IDS) sensors at critical points in the network to detect and alert in case of unauthorised attempt to access Document Cloud. Additionally, Document Cloud operations teams continuously monitor sensitive logs and conduct periodic system audits to help ensure that inappropriate access to critical assets does not occur.

As much as possible, Adobe automates processes and procedures to help create efficiencies, maintain consistency and repeatability, and reduce human error. Document Cloud uses automation in areas including configuration and patch management, creation and hardening of baseline images, and system monitoring. Adobe enforces a comprehensive, change management process to help ensure that changes to the network or Document Cloud production environment are documented, tracked, tested, authorised and approved prior to migration to production.

When an incident occurs with an Adobe cloud-based service, including Document Cloud, Adobe centralises incident response, decision-making, and external monitoring in its Security Coordination Centre (SCC), providing cross-functional consistency and fast resolution of issues.

Internal and third-party testing and assessments

New product features are reviewed for design flaws that impact security, and security testing is integrated into the application development lifecycle. Additional vulnerability testing is conducted in the form of source code reviews and static and dynamic analysis scans. Every major Document Cloud service release is subjected to independent third-party application penetration testing prior to release and critical bugs are addressed prior to release.

Compliance

Document Cloud services are compliant with ISO 27001:2013, PCI DSS* and SOC 2 Type 2 and meet many additional industry-specific compliance certifications, standards and regulations. For example, Adobe Sign is SAFE-BioPharma® certified and complies with HIPAA, FERPA, GLBA and 21 CFR Part 11.

Access control

Document Cloud infrastructure resides in top-tier data centres managed by our trusted cloud service provider Amazon Web Services (AWS). Adobe uses role-based access control methods that restrict privileged access to information resources based on the concept of least privilege. Authorisation to access requires approval by the management directly responsible for the confidentiality, integrity and availability of impacted resources. Only approved, authorised Adobe employees, cloud service provider employees and contractors with a legitimate, documented business are allowed access to the secured sites in North America, the European Union, Australia and Japan.

For more information

Adobe security:
www.adobe.com/uk/security.html

Adobe privacy:
www.adobe.com/uk/privacy.html

* PCI DSS compliance excludes the Adobe Send & Track service.

Adobe

Adobe Systems Europe Ltd
Market House, 34-38 Market Street,
Maidenhead, SL6 8AD
United Kingdom
www.adobe.com, www.adobe.com/uk

10/17