Adobe® Connect™ Managed Services

Security overview

Adobe Connect Managed Services provides a comprehensive offering of Adobe Connect as a managed service. Adobe, together with its hosting partner Amazon, provides a broad array of security elements mixed into the offering in order to provide a secure foundation upon which the customer can build their solution. Combined with security-aware customization, testing, and monitoring, these elements form the basis for a highly secure yet easy-to-use solution.

Physical security

Amazon data centers are housed in state of the art, but nondescript, facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass a rigorous authentication process, including biometric scanning and mantraps to access data center floors. All visitors and contractors are required to present identification, are signed in, and continually escorted by authorized staff.

Amazon only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked.

All physical access to data centers is logged and audited routinely.

Network security

Adobe Connect Managed Services provides a firewall as a part of its standard solution offering. Ports are shut down by default and our customers are able to select only that which they need to allow the specific inbound traffic to meet their needs. Traffic may be restricted by service port, as well as by source IP address.

Adobe further secures instances through the use of reverse proxy systems in front of web servers to further enhance security. These reverse proxies are based upon the asynchronous event-driven approach for more predictable performance under load.

Adobe provides SSL certificates for all Production systems and highly recommends that customers take advantage of this security model whenever possible. Adobe also provides a variety of other communication options for the customer to implement as required during the customization of the solution.

Data security

The first layer of data protection is simply that Adobe Connect Managed Services are hosted on dedicated single-tenant virtual machines using hypervisor-protected virtualized disks and other resources. This prevents other customers from inadvertently (or otherwise) accessing customer data, processes, or runtime environment on the machine. Customers, as well as Adobe, are prevented from accessing the underlying physical machine and Amazon is prevented from accessing the virtual machines from the underlying server.
Adobe encrypts all customer data, which is stored in either the solution database or elsewhere on the Elastic Block storage system. This encryption is done using AES 256-bit keys for maximum data storage protection. This encrypted data is likewise routinely backed up in an encrypted fashion. The encrypted backup data is stored in small data packets across the highly available storage access system and considerable file knowledge is required to reassemble the encrypted backup files.

When a backup file is no longer required, the file is released, deleted, and overwritten by other customer data almost immediately, making for a very secure endgame. Adobe customers that require that all data be wiped via a specific method, such as DoD 5220.22-M or NIST 800-88, should indicate this to Adobe, so that their solution may be developed with these wipe procedures in mind.

Access security
Adobe follows a specific practice to secure the calls to the Amazon Web Services infrastructure. Calls that launch and terminate instances, change firewall parameters, and perform other functions are all signed by the Adobe EC2 Secret Access Key. Likewise, calls to the mass data storage system must be signed by the Adobe EBS/S3 Secret Access Key. Employee access to Adobe’s Amazon accounts is always done using three-factor authentication with special OTP dongles provided by Amazon. Without access to these keys, instructions cannot be given to change any of the parameters in the Adobe infrastructure at Amazon. Access to instance and environmental monitoring is controlled through a separate set of passwords. Development and testing of instances is done through Amazon accounts which are fully separated from Production accounts.

All Adobe systems use network address translation processes which link the internal IP address of the customer instance with a dedicated, publicly-facing IP address that is used for all public communications with the system.

All Adobe Connect Managed Services use dedicated domain names (e.g. custx.acms.com) provided and managed by Adobe that are linked to the system’s publicly-facing load balancers and IP addresses. The customer may, by special request, also choose to use URLs of their own associated with the solution, either under their own management or Adobe’s—though special arrangements are required.

Access to the underlying instances is under strict control by Adobe at all times to help ensure that only authorized users can access the system.

To minimize the risk of system compromise during the promotion of an environment to production status, Adobe uses a series of access controls provided to the customer and partners during development. Once the service goes to Production status, Adobe removes all access to the underlying system except that which is specifically needed by the customer for solution operation. Customer and customizer access is revoked and any shared passwords for the underlying system, except those used for routine monitoring, are changed. Likewise, Adobe employee access is heavily controlled and employees are only allowed system access for the purposes of upgrade, troubleshooting, and incident response. In the case of the incident response teams, the passwords are again changed once the system access event is closed.

Security reviews
The Adobe Connect Managed Services system is governed by a comprehensive set of documented security processes and has been subject to numerous security audits.

As noted above, our systems are hosted on the Amazon Elastic Compute Cloud, which has been subject to numerous reviews and audits. Perhaps most relevant to this discussion are Amazon’s ISO27001 and ISO27002 certifications. A Statement on Auditing Standards for service providers provides a complete review by an independent auditor of both certifications:

- The service auditor’s opinion on the service organization’s description of controls that have been placed in operation
- The auditor’s opinion on the fairness of the presentation of the service organization’s description of these controls
Adobe has received and reviewed the auditor's extensive report on the above and is satisfied with the findings.

Adobe's service is also under continuing review to ISO27001 standards. Adobe is currently in phase one, self audit, of the ISO27001 process and expects to be fully compliant with ISO27001 standards in the future.

For more information
Amazon Web Services:
Overview of Security Processes

Product details:
www.adobe.com/products/adobeconnect

For more information on Adobe systems and controls, please contact your Adobe sales representative or partner. Further details on the Adobe solution, including SLAs, change approval processes, Runbook management and samples, access control procedures, and disaster recovery processes are available.