Adobe® Experience Manager Managed Services

Security overview

Adobe Managed Services provides a comprehensive array of measures targeted at securing instances of Adobe Experience Manager in four key areas: physical, network, data, and access security. These measures provide a secure foundation on which enterprises can build their business-critical websites and manage their digital assets.

Physical Security	Network Security	Data Security	Access Security
• World-class access-control security • Limited access to data centers • Rigorous authentication processes	• Constant traffic monitoring • Built-in firewalls inside Experience Manager • Secure Sockets Layer (SSL) certificate support • Custom security options	• Dedicated, single-tenant virtual machines • Encrypted, highly available storage and backups • Secure data wipe	• Commands to Amazon cloud require multiple levels of authentication • Access to production system limited and strictly controlled

Adobe Experience Manager Managed Services provides a comprehensive array of security measures:

- Professional physical security
- Carefully designed network security
- Encrypted data
- Strictly enforced access security
- Regular security reviews

Physical security

Hosted on the Amazon Web Services (AWS) platform, Adobe Experience Manager Managed Services leverages Amazon's experience in designing, constructing, and operating large-scale data centers. The AWS data center security measures include:

- Nondescript, state-of-the-art facilities
- Strictly controlled physical access by professional security staff via video surveillance, physical intrusion detection systems, and other electronic means
- Limited access to facilities granted to employees and contractors who have a legitimate business need only during the time that the need exists
- Rigorous authentication process to access the data center floors, supported by mantraps and constant escort for those with a need for access
- Separation of responsibilities so that those with physical access to the servers do not have electronic access to the servers
- Continual logging and auditing of access to data centers

Network security

To enable customers to build geographically dispersed, fault-tolerant web architectures with cloud resources, Adobe and AWS provide a carefully monitored and managed world-class network infrastructure, including:

- Network monitoring and protection—AWS uses a variety of automated monitoring systems to provide a high level of service performance and availability.
- Secure network architecture—Data flows are controlled and managed through boundary devices and traffic flow policies.
- Transmission protection—Servers can be accessed only through HTTP or secure protocols, unless otherwise requested by the customer.
- Security groups—Access is controlled by IP address, port, and protocol on a server-by-server basis.
- Virtual private cloud—Available upon request, deployments provide a VLAN-type infrastructure and a termination point for customer-originating VPNs.

Additionally, Adobe provides SSL certificates for its standard URLs for all development systems. Adobe strongly encourages customers to use SSL whenever possible. Adobe can support a customer-supplied SSL certificate, if desired.

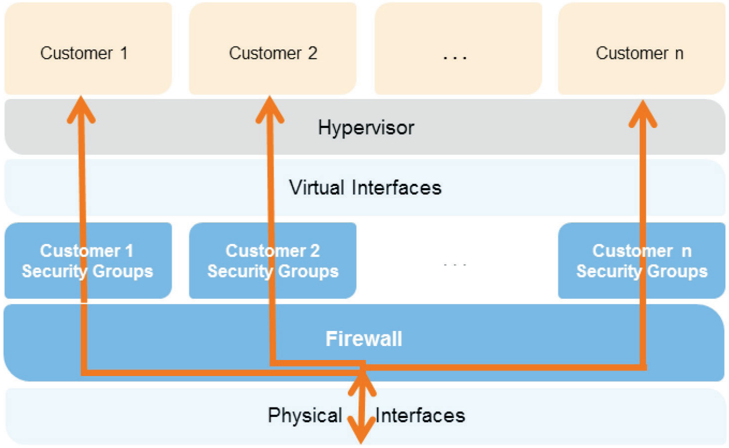
Adobe can also support implementing a variety of other secure communication options as required during the customization of the solution.

Data security

AWS and Adobe place a high emphasis on protecting customer data and backups while providing maximum availability and data integrity.

Experience Manager deployments are hosted on dedicated, single-tenant virtual servers. This architecture prevents other Amazon customers from inadvertently (or otherwise) accessing customer data, processes, or the runtime environment on the machine. Customers and Adobe are prevented from accessing the physical machine, while Amazon is prevented from accessing the virtual machines from the underlying server.

As a part of the commitment to the security of the solution deployed in the cloud, AWS provides a complete firewall solution which comes as a mandatory inbound firewall configured in a default deny-all mode and Amazon EC2 customers must explicitly open the ports needed to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block). The firewall administration requires a X.509 certificate and key to authorize changes, thus separating the firewall from the application instances and adding an extra layer of security.



Amazon cloud, multiple layers of security

Customer backups and content, or other data present on the author and publish nodes, can be stored on Amazon Elastic Block Storage (EBS) or Amazon Simple Storage System (S3), which are outside of the system described above. EBS features:

- Encryption—All data stored on the system uses 256-bit key encryption.
- Routine backups—Encrypted backups are stored in small data packets across the highly available storage system with virtually no possibility for reassembling the data without considerable knowledge.
- Backup distribution—Backups are automatically distributed in an encrypted format to alternate availability zones within the customer-specified cloud region to enable emergency recovery.
- Secure backup disposal—Backups are released, deleted, and overwritten immediately when they are no longer needed. When the contract is terminated, all security keys are destroyed, and active instances are terminated.

Amazon S3 provides a higher uptime availability and capacity than EBS along with some differences in features:

- Encryption—"Server-side Encryption" ensures that all data in S3 is stored encrypted using AES-256 keys (on a per object basis), which are themselves encrypted by a master key which itself is automatically rotated by Amazon every month. Further, S3 bucket policies ensure that only the designated AEM user gets access to the bucket's contents.
- Backups are automatically distributed by Amazon in an encrypted format to alternate availability zones within the customer-specified cloud region. Additional AWS regions can be added as an option.

Access security

Adobe follows a secure practice in securing access to the AWS infrastructure and customer Experience Manager instances.

- AWS access—Calls that launch and terminate instances, change firewall parameters, or access EBS are all signed by Adobe secret access keys.
- Adobe's Amazon accounts—Employee access must use three-factor authentication using Adobe corporate identity, AWS OTP, and Adobe network communications origins.
- Experience Manager Managed Services—Public access can be either Adobe-provided domain names, such as custx.adobecqms.com, or URLs provided by the customer.
- Experience Manager instances—Access to the underlying instances is under strict control by Adobe at all times to ensure that only authorized users can access the system. Prior to production, Adobe controls system access by partners and the customer to minimize the risk of system compromise. When in production, Adobe removes all access to the production solution, except the access needed for solution operation. Adobe employee access is tightly controlled, and a limited number of employees are only allowed system access for the purposes of upgrades, troubleshooting, and incident response, with passwords changed when the access requirement is closed.

Security reviews

Adobe Managed Services system is governed by a comprehensive set of documented security processes and has been subject to numerous security audits to maintain and improve the quality of our services. Experience Manager Managed Services is hosted on the Amazon Elastic Compute Cloud (EC2), which has been subject to numerous reviews and audits for compliance with Amazon's SAS 70 Type II and ISO27001 certifications. Adobe Managed Services is also under continuing self-review to ISO 27001 standards and in the process of achieving Authority to Operate under FedRAMP-moderate as well as HIPAA certification, although extra fees and extended timelines may apply for customers requiring these additional levels of security.

For more information

Adobe Managed Services team members are available to address requests for more information. Detailed AWS security documentation is available per signing a nondisclosure agreement with AWS. Based on the customer need, AWS staff is available to join client meetings and answer questions and address security concerns.

For more information
www.adobe.com/solutions/web-experience-management.html

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com