Adobe® Creative Cloud for enterprise Security Overview

Table of Contents

Executive Summary

At Adobe, we take the security of your digital assets seriously. From our rigorous integration of security into our internal software development process and tools to our cross-functional incident response teams, we strive to be proactive and nimble. What's more, our collaborative work with partners, researchers, and other industry organizations helps us understand the latest threats and security best practices as well as continually build security into the products and services we offer.

We built Adobe Creative Cloud for enterprise with security considerations at its core, and we utilize industry-standard software security methodologies for both development and management of the Creative Cloud for enterprise solution. From desktop and mobile apps to cloud services, your assets are protected, managed, and monitored by state-of-the-art security.

Adobe services that touch customer content have completed multiple standards certifications. Please see the Current List of Certifications, Standards, and Regulations for a detailed list of all compliance certifications and standards, as well as government regulations currently supported by Adobe products and solutions. For information on GDPR, please see the Adobe GDPR Readiness page.

This whitepaper describes the proactive approach, as well as procedures and security architecture, implemented by Adobe.

Creative Cloud for enterprise Overview

Creative Cloud for enterprise is a modern creative platform for businesses that want to design stand-out experiences across devices and customer touchpoints. With a collection of desktop and mobile apps, built-in templates, and cloud services, Creative Cloud for enterprise unlocks the content velocity required for today's digital transformation.

Desktop Applications

Packaged for deployment by IT via standard methods, such as Microsoft SCCM/JAMF Casper Suite, or utilized in a self-service scenario in which end-users download the apps directly from Adobe, Creative Cloud for enterprise desktop apps run on the end-user's desktop system. Each user is assigned a desktop application license via the Admin Console based on their identity (see User Authentication section below). When a user launches a Creative Cloud for enterprise app, such as Photoshop, the app communicates with Adobe Identity Services to determine if the user is entitled to use that application. Adobe encrypts all Creative Cloud data transmissions and handles user information by applying industry standards and best practices for security and privacy.

Mobile Apps

Adobe mobile apps run on users' mobile devices (including smartphones and tablets) and may be managed by a Mobile Device Management (MDM) solution. Content created by any of the mobile applications is stored both on the mobile device and in the cloud using encrypted storage (see the Cloud Services section below). Data transmissions are encrypted and access to the mobile services is determined by user identity as configured in the Admin Console. Adobe also leverages tooling to regularly scan and secure our mobile applications. This helps ensure they are following security best practices and properly leveraging the security controls provided by their underlying operating systems.

Cloud Services

Cloud services available in Adobe Creative Cloud for enterprise include a variety of productivity features that increase the efficiency of users. Using the Admin Console, administrators entitle users for Creative Cloud for enterprise services, including those that enable designers to access files, collaborate on projects, and leverage multiple fonts and stock images. Access to services is based on each user's unique identification, which means that only users entitled to a service may access it.

All data transmissions are encrypted and user generated content (UGC) is encrypted at-rest. As detailed in the *Dedicated Encryption Key* section below, both transmissions and UGC may be additionally encrypted with a dedicated encryption key.

Admin Console

The Adobe Admin Console is used to manage named user accounts as well as to configure license and service entitlements. It provides role-based access to Creative Cloud for enterprise apps and services and enables user management and entitlement access to Adobe Document Cloud, Adobe Marketing Cloud, and Print & Publishing applications. IT staff can also utilize the Admin Console to open support cases with Adobe Customer Care or schedule Expert Services sessions, so they can quickly resolve problems and issues.

Not only does the Admin Console integrate with any SAML 2.0-compliant enterprise identity management system for authentication, but it also works with the different ID types described in the *Entitlement and Identity Management* section below.

IT staff can set up product license groups to either mirror the enterprise directory groupings or create separate groups specifically tied into creative workgroups. Additionally, Adobe exposes a user management API that enables administrators to quickly configure license and service entitlements. The API also allows the admin to revoke all content access, if required.

If needed, the Admin Console can control a customer-specific, dedicated encryption key that encrypts all cloud content with a FIPS 140-2-compliant key utilizing envelope encryption. The Admin Console also allows administrators to view logs of all uploaded content as well as restrict the ability of end-users to share cloud content with anyone outside of the organization.

Administrators can download detailed reports, called content logs, from the Admin Console. These reports give information on how end-users are working with corporate assets. As end-users interact with the assets (e.g., create, update, etc.) the details are recorded in log files. Administrators can export these log files to track actions that users perform on the Creative Cloud assets owned by an organization. Logs can be generated for user activities that occurred in the past 90 days.

All communication with the Admin Console is encrypted using AES 128-bit GCM for symmetric key cryptographic block ciphers over TLS 1.2. Administrator access is limited to assigned users, which are set up and controlled by the customer.

Enterprise Storage Management

Enterprise Storage Management (ESM) is an update to Adobe storage that provides users with more control, insight, and security over their Creative Cloud for enterprise accounts. In addition to pooling storage allocation at the organizational rather than the individual level, ESM also enables Creative Cloud for enterprise administrators to:

- Run per-user storage reports and generate alerts on a storage dashboard when a user exceeds their granted storage limit
- Reclaim assets by transferring one employee's cloud content to another employee
- Designate a storage administrator whose sole role is to handle storage administration tasks

Currently, ESM does not enable individuals to manage their own storage quota or provide a mechanism to entirely prohibit cloud data storage.

Creative Cloud for enterprise Identity Systems

Entitlement and Identity Management

IT administrators entitle end-user access to Creative Cloud for enterprise desktop applications, such as Adobe Photoshop and Adobe Illustrator, as well as to cloud services, by utilizing named user licensing in the Adobe Admin Console. There are three (3) enterprise ID management options:

- **Adobe Business ID** is an Adobe-hosted, enterprise-managed option for organizations that either use email addresses outside of their own claimed domain as the user's ID or for customers that have not claimed a domain for identity purposes. Adobe Business ID is the preferred option for organizations that work with outside contractors or freelancers who do not have an organizational ID or email. With a Business ID, enterprises can separate users' business content from their personal content and can control and manage all business content created by the user (up to 2TB storage each).
- **Adobe Enterprise ID** is an Adobe-hosted, enterprise-managed option for organizations that use email addresses inside their own domain. The accounts are created and controlled by IT administrators from the customer enterprise organization, and the organization owns and manages both the user accounts and all associated assets. While a Business ID does not require a user to login with an email address from the organization's claimed domain, an Enterprise ID does.
- **Adobe Federated ID** is a Single-Sign-On (SSO) identity in which identity profiles are provided by the customer's identity management system. Federated IDs and associated assets are created, owned, and controlled by the customer's IT department. Adobe integrates with most any SAML 2.0-compliant identity provider. See the steps used to migrate to a customer identity provider at https://helpx.adobe.com/enterprise/using/set-up-identity.html

Application and service entitlement for any of the above methods is managed using the Adobe Admin Console.

Most enterprise organizations use Federated IDs for their employees and use Business IDs for their contractors and freelancers. You can learn more about each identity type at https://helpx.adobe.com/enterprise/help/identity.html.

For more information about Adobe's security practices for identity services, please see: https://www.adobe.com/content/dam/acom/en/security/pdfs/AdobeIdentityServices.pdf

Password Lockout Procedures

Organizations can enforce password policies for both Business IDs and Enterprise IDs with three (3) different password policies, shown here:

Domain Claims | **Password Requirements**

Password Requirements:	Level IV	Level V	Level VI
Minimum Number of Characters	✓ (8+)	✓ (8+)	✓ (8+)
Symbol & Number	✓ (1+ of both)	✓ (1+ of both)	✓ (1+ of both)
Lower & Upper Case Characters	✓	✓	✓
Cannot Match Previous Passwords	✓ (last 5)	✓ (last 5)	✓ (last 5)
Expiration	X	✓ (90 days)	✓ (90 days)

Creative Cloud for enterprise password policies

Both Business IDs and Enterprise IDs leverage the SHA-256 hash algorithm in combination with password salts and a large number of hash iterations. Adobe continually monitors accounts hosted on its infrastructure for unusual or anomalous account activity and evaluates this information to help quickly mitigate security threats. Conversely, Adobe does not manage user passwords for Federated ID accounts.

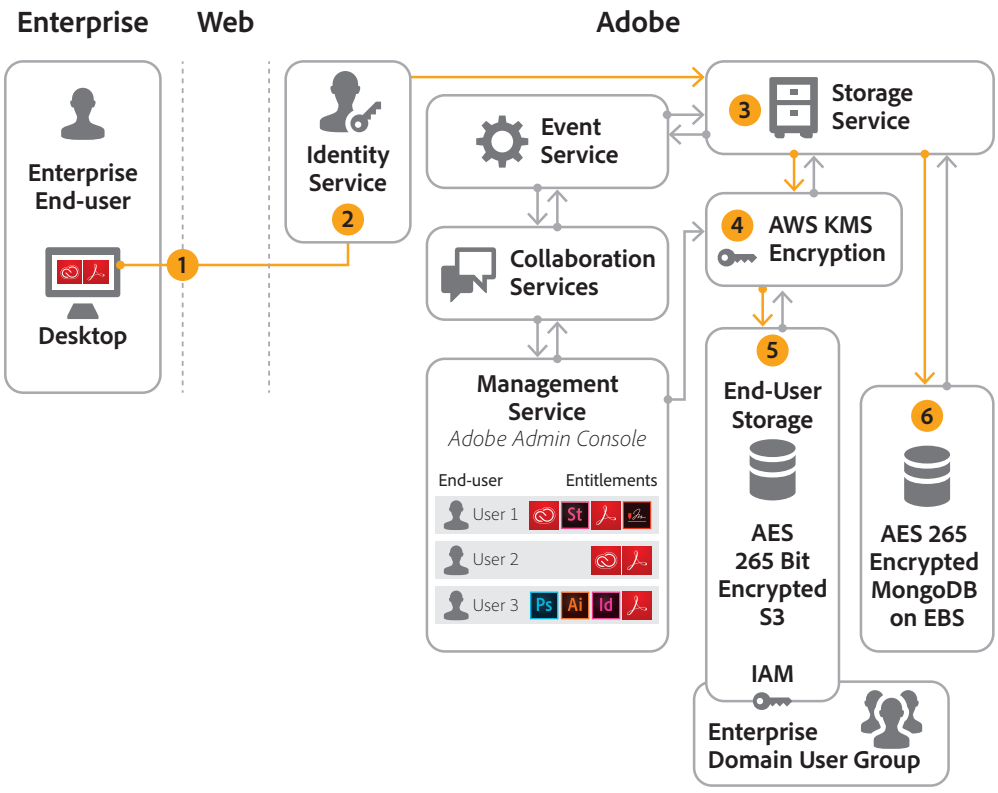
Account Management

IT departments can create, manage, and delete Business ID, Enterprise ID, and Federated ID accounts through the Adobe Admin Console. Cloud storage for these accounts is allocated as individual storage, which means IT staff does not have direct access to any files in the user's Creative Cloud for enterprise storage. However, IT staff may assume ownership for the employee's account and revoke access or, with ESM, remove a user and transfer their assets to another user.

Removing a user either involves removing entitlements for that user or completely deleting the user account. Removing the entitlements of a user with existing shared services storage renders any data in cloud storage inaccessible to that user and prohibits them from using the desktop applications, but it does not delete the user or their cloud content. Completely deleting a user removes that user from the Admin Console and deletes their data. A deleted user's data is erased from disk 14 days after their account is deleted.

Creative Cloud for enterprise Solution Architecture and Data Flow

Creative Cloud for Enterprise User Generated Content Data Flow

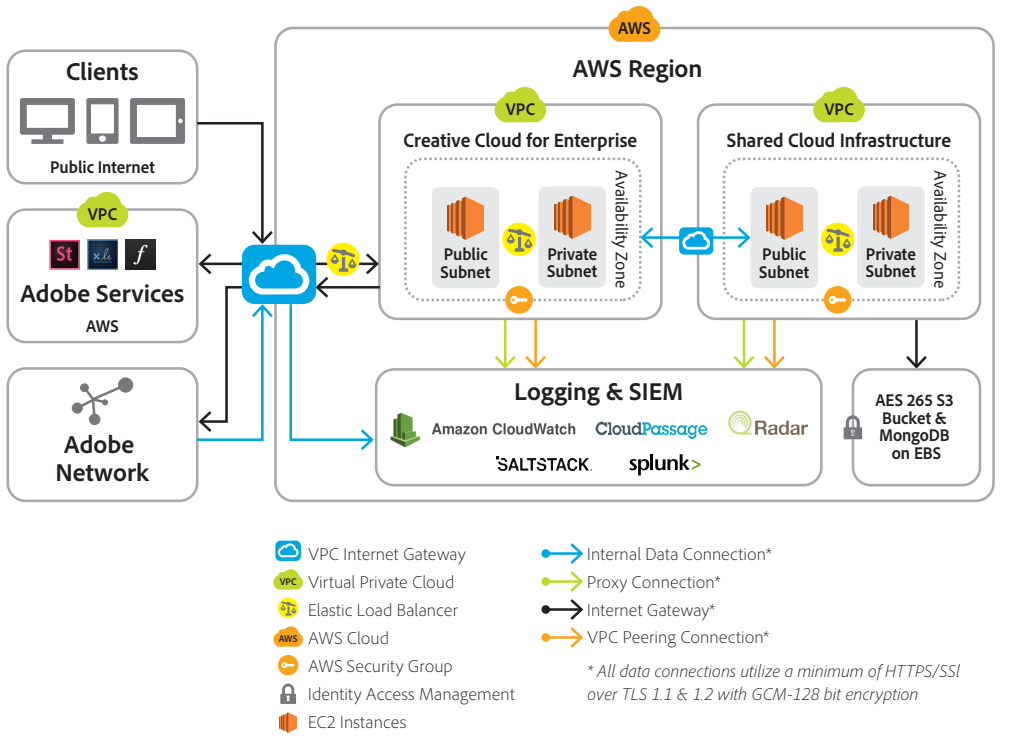


Creative Cloud for enterprise UGC data flow

1. End-users store the content they create in a Creative Cloud folder on their system's hard drive. If the user chooses to upload this content to cloud storage in Creative Cloud for enterprise, a background process uploads the UGC to the cloud. All UGC is encrypted in-transit using AES 128-bit GCM over TLS 1.2.
2. The Adobe Identity Service validates the user and their entitlements.
3. Adobe Creative Cloud for enterprise scans the content for viruses and sends the content to the AWS Key Management System (KMS) for encryption.

4. AWS KMS encrypts the user's content with the customer-managed encryption key. For more detail on KMS, go to http://aws.amazon.com/kms/faqs/.
5. Creative Cloud for enterprise stores the encrypted content in AES 256-bit Amazon S3 storage. In order to update or retrieve the content, the user must use Creative Cloud for enterprise; there are no external links to the content.
6. Metadata about the content is stored in MongoDB on an Amazon EBS using AES 256-bit encryption.

Creative Cloud for enterprise Solution Architecture



Creative Cloud for enterprise solution architecture

Creative Cloud for enterprise leverages multi-tenant storage in which customer content is processed by an Amazon Elastic Compute Cloud (EC2) instance and stored on a combination of Amazon Simple Storage Service (S3) buckets and through a MongoDB instance on an Amazon Elastic Block Store (EBS).

Creative Cloud for enterprise is deployed regionally, as noted in the Data Center Locations and Your Data section below. Each region contains two VPC (Virtual Private Cloud) instances, a Creative Cloud for enterprise VPC and a Shared Cloud VPC. Both VPCs are logically isolated networks within an AWS region.

The Creative Cloud for enterprise VPC hosts the websites and APIs where end-users interact with the solution, and the Shared Cloud VPC hosts the services that perform common tasks across Creative Cloud for enterprise, such as storage.

In practice, availability zones exist as isolated locations within a region. However, from a network architecture perspective, they reside in a VPC. Physically, each availability zone has multiple different redundant data centers, enabling all data to be replicated across all data centers as well as within multiple servers within each data center. This redundant backup ensures that Creative Cloud for enterprise customer data is safe from disasters, floods, power failures, etc.

Everything within each VPC is locked down by an AWS Security group, represented by orange keys in the chart above. A security group is another layer of security that allows Adobe to control the inbound and outbound traffic through the VPC, much like a virtual firewall.

The actual code within the VPC is housed in Amazon EC2 instances in specific subnets (or ranges of IP addresses). While public subnets are connected to the internet, private subnets are not and are only accessible through authenticated connections originating from the public subnet. This prevents an

unauthorized user from connecting directly to the Creative Cloud for enterprise storage service, for example, and allows Adobe to make sure that only authorized users can perform certain actions, such as storing UGC.

UGC is stored in Amazon S3 buckets and the metadata about the content is stored in Amazon EBS via MongoDB. The UGC is then protected by Identity and Access Management (IAM) roles within that AWS region. Implementing per-user content security, IAM roles ensure that any content an end-user uploads to the cloud is considered private and is only accessible by that user, unless they take explicit steps to share it.

Content and assets stored in S3 are encrypted with AES 256-bit symmetric security keys that are unique to each customer and their claimed domain. The dedicated keys are managed by the Amazon Key Management Service (KMS), which provides additional layers of control and security for key management. Adobe automatically rotates the key on an annual basis. If necessary, IT administrators can revoke their key via the Admin Console, which will render all data encrypted with that key inaccessible to end-users. For more information, see the below section on dedicated encryption keys.

Metadata and support assets are stored in EBS using AES 256-bit encryption and Federal Information Processing Standards (FIPS) 140-2 approved cryptographic algorithms, both of which are consistent with National Institute of Standards and Technology (NIST) 800-57 recommendations.

For more information on Adobe's cloud services compliance, please see: https://www.adobe.com/content/dam/acom/en/security/pdfs/AdobeCloudServices_ComplianceOverview.pdf

For more information on Adobe's secure software engineering practices, please see: https://www.adobe.com/content/dam/acom/en/security/pdfs/adobe-secure-engineering-wp.pdf

For more information on the underlying Amazon services, please see:

- MongoDB: http://www.mongodb.org
- Amazon S3 service: https://aws.amazon.com/s3/faqs
- Amazon KMS service: http://aws.amazon.com/kms/faqs/
- Amazon EC2 service: http://aws.amazon.com/ec2/

Data Center Locations and Your Data

User generated content is redundantly stored in multiple data centers within a region and on multiple devices in each data center. All network traffic undergoes systematic data verification and checksum calculations to prevent corruption and ensure integrity. Finally, stored content is synchronously and automatically replicated to other data center facilities within the customer's region so that data integrity is maintained even in the event of data loss in two locations.

UGC created using Creative Cloud for enterprise can be stored in the US (US-East VA), Europe (EMEA-West IE), or Japan (APAC-West JP) regions. An end-user's regional data store is determined when the user is created in the Adobe Admin Console and remains consistent throughout the user's lifetime. In other words, content created by a user account in the US will always be stored in the US data center, regardless of where the user is located when they upload the content.

Dedicated Encryption Key

As mentioned above, Adobe encrypts all UGC stored in Creative Cloud for enterprise at rest. For an additional layer of control and security, IT administrators can enable a dedicated encryption key for some or all the domains in the organization. Content is then encrypted using that dedicated encryption key which, if required, can be revoked from the Admin Console. Revoking the key will render all content encrypted with that key inaccessible to all end-users and will prevent both content upload and download until the encryption key is re-enabled.

The key service employed utilizes FIPS 140-2 validated hardware security modules (HSMs) to protect key integrity and confidentiality. Plain-text keys are never written to disk and are only used in the HSM volatile memory on the server in the regional data store.

For more information on managing encryption using a dedicated key, please see:

- https://helpx.adobe.com/enterprise/help/encryption.html
- https://helpx.adobe.com/enterprise/help/encryption-faq.html

Creative Cloud for enterprise Content Sharing and Collaboration

All Creative Cloud for enterprise content stored in the cloud is automatically labeled "Private," which means the content is only visible to the end-user who uploaded it. The user must take explicit actions to share content or it will remain private. Sharing in Creative Cloud for enterprise is accomplished in the following two ways:

Collaborate

Collaborated content remains private and the content owner must specifically invite named recipient/s to view or edit the content. Only the invited recipients can view the content and the collaborators must authenticate themselves to view it. If any collaborator changes the content, all collaborators can view the changes. Collaborated content in the cloud physically remains in the regional data center of the content owner—it is never relocated to a collaborator's regional storage.

A user can only be invited to collaborate on a Creative Cloud (CC) Folder, CC Library, or certain Cloud Documents. Individual pieces of content within a shared CC Folder or CC Library are accessible by the invited collaborator but CC Collaboration is at the folder or "group" level. Adobe Experience Design (XD) Prototypes and Design Specs are also enabled for CC Collaboration.

If a user wants to share an individual file or a mobile creation, they must use the "Send Link" function instead.

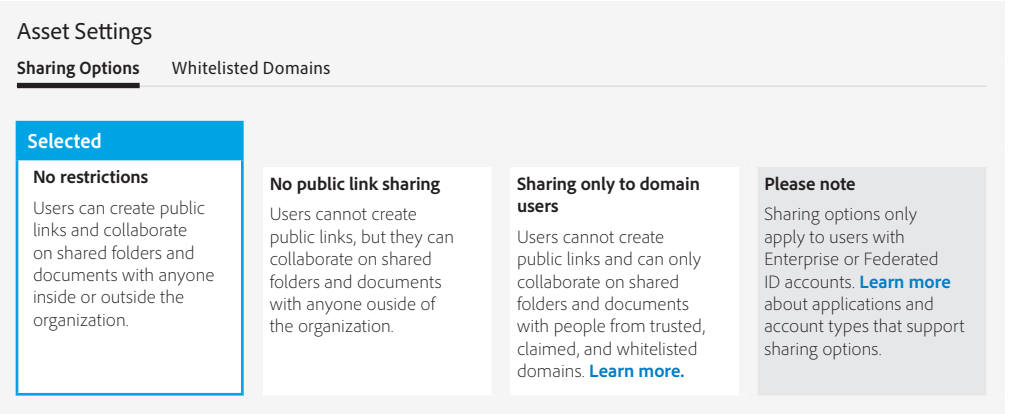
Send Link

Creative Cloud for enterprise also gives users the ability to share content with other users through the "Send Link" option. Unlike collaboration, sending a link creates a public link to the content and anyone with that link address can view the content. Linked content can be shared with the option to "Allow Download" or "Allow Save" which, if enabled, allow the recipient to download the content to either their desktop or their own Creative Cloud storage. In either case, the connection to the original content is broken and the recipient is now considered to be the owner of the content, with that content residing in the recipient's assigned data center.

When sending a link to a CC Library, the "Allow Follow" option enables recipients to access a read-only view of the CC Library and receive any updates made by the owner. Unless downloaded as noted above, a "followed" CC Library will remain in the data center of the owner.

The ability to perform a Send Link on content can be controlled by the enterprise administrator using the **Asset Settings** feature in the Admin Console.

Asset Settings and Sharing Restrictions



Administrators can manage sharing restrictions for content stored in Creative Cloud for enterprise using the Asset Settings feature in the Admin Console.

Enterprise IT departments can turn off public link sharing and limit collaboration to the enterprise-claimed domain and any other whitelisted domains. Limiting collaboration to claimed domains means that designers can only share content with other users within their organization; external sharing is completely disabled.

Access Request Policy

Administrators can also choose between two (2) access request policies:

- **Allow access requests** — The default setting, "Allow access requests," allows users to request access to folders or documents that have not been specifically shared with them. Users with sharing permissions on the asset receive notifications for each access request and can decide whether to grant access or not.
- **No access requests** — For added privacy, administrators can prevent users from being able to request access to a document that has not been specifically shared with them.

Hosting Services

All components of Creative Cloud for enterprise are currently on Amazon Web Services (AWS),

including Amazon EC2 and Amazon S3, in the United States, the European Union (EU), and Asia Pacific. Amazon EC2 is a web service that provides automatically scalable compute capacity in the cloud, making web-scale computing easier. Amazon S3 is a highly reliable data storage infrastructure for storing and retrieving any amount of data.

The AWS platform provides services in accordance with industry-standard practices and undergoes

regular industry-recognized certifications and audits. You can find additional information about AWS and Amazon's security controls on the AWS security site and can obtain a SOC 2 report by entering into an NDA with AWS.

Operational Responsibilities of AWS and Adobe

As the hosting provider, AWS operates, manages, and controls components from the hypervisor virtualization layer down to the physical security layer of the facilities in which Adobe Creative Cloud for enterprise runs. In turn, Adobe assumes responsibility for and management of the guest operating system (including updates and security patches) and application software, as well as the configuration of the AWS-provided security group firewall.

AWS also operates the cloud infrastructure used by Adobe to provision a variety of basic computing resources, including processing and storage. The hosting infrastructure includes facilities, network, and hardware, as well as the operational software (e.g., host OS, virtualization software, etc.) that support

the provisioning and use of these resources. Amazon designs and manages the hosting environment according to industry-standard practices as well as a variety of security compliance standards.

Secure Management

Adobe uses Secure Shell (SSH) and Secure Sockets Layer (SSL) for management connections to manage the hosting infrastructure.

Geographic Location of Customer Data on AWS Network

The following information is from the AWS: Overview of Security Processes White paper. For more details, please consult the AWS white paper.

Identity data is stored in multi-region, load-balanced, AWS data centers located in US-East (Virginia), US-West (Oregon) and EU-West (Ireland). Content is backed up within each data center, in other data centers within the region, and in cross-region data centers for load balancing and redundancy. Adobe complies with applicable laws regarding cross-border data transfers, as outlined in greater detail at https://www.Adobe.com/privacy/eudatatransfers.html.

UGC uploaded to Creative Cloud for enterprise is generally stored in the AWS regional data center that corresponds to the country code associated with the user uploading the data, regardless of identity type:

- UGC for users with a North American, Central American or South American country code is stored in the AWS US-East 1 (Virginia) data center
- UGC for users with a European or African country code is stored in the AWS EU – West 1 (Dublin, Ireland) data center
- UGC for users with an Asia-Pacific or Middle Eastern country code is stored in the AWS – Asia Pacific Northeast 1 (Tokyo) data center

Isolation of Customer Data/Segregation of Customers

AWS uses strong tenant isolation security and control capabilities. As a virtualized, multi-tenant environment, AWS implements security management processes and other security controls designed to isolate each customer from other AWS customers. Adobe uses AWS Identity and Access Management (IAM) to further restrict access to compute and storage instances.

Secure Network Architecture

AWS employs network devices, including firewall and other boundary devices, to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to manage and enforce the flow of traffic. The Amazon Information Security team approves all ACL policies and automatically pushes them to each managed interface using the AWS ACL-Manage tool, helping ensure these managed interfaces enforce the most up-to-date ACLs.

Network Monitoring and Protection

AWS uses a variety of automated monitoring systems to provide a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities and conditions at ingress and egress communication points. The AWS network provides significant protection against traditional network security issues:

- Distributed Denial of Service (DDoS) attacks
- Man-in-the-Middle (MITM) attacks
- IP spoofing
- Port scanning
- Packet sniffing by other tenants

You can find more information about network monitoring and protection in the AWS: Overview of Security Processes white paper.

Intrusion Detection

Adobe actively monitors Adobe Creative Cloud for enterprise using industry-standard Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Adobe uses Hubble, an in-house developed tool, run on all servers, which includes File Integrity Monitoring, checking critical aspects of the filesystem, connections, running processes, and running state of the systems. Scans are performed in real-time and continuously run scanning for malware and other malicious activity.

Logging

Adobe conducts server-side logging of Adobe Creative Cloud for enterprise customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs only store Business IDs to help diagnose specific customer issues and do not contain username/password combinations. Only authorized Adobe technical support personnel, key engineers, and select developers can access the logs to diagnose specific issues that may arise.

Service Monitoring

AWS monitors electrical, mechanical, and life support systems and equipment to help with the immediate identification of service issues. In order to maintain the continued operability of equipment, AWS performs ongoing preventative maintenance.

Data Storage and Backup

Adobe stores all Adobe Creative Cloud for enterprise content in Amazon S3 and metadata in a MongoDB database on Amazon EBS, both of which provide a storage infrastructure with high durability. To help enhance this durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities and redundantly store objects on multiple devices across multiple facilities in an Amazon S3 region.

In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. Metadata is replicated by taking snapshots of Amazon EBS volumes and stored regionally, similar to how content is stored in Amazon S3. Data replication for Amazon S3 data objects occurs within the regional cluster where the data is stored and is not replicated to data center clusters in other regions.

Change Management

AWS authorizes, logs, tests, approves, and documents routine, emergency, and configuration changes to existing AWS infrastructure in accordance with industry norms for similar systems. Amazon schedules updates to AWS to minimize any customer impact. AWS communicates with customers either via email or through the AWS Service Health Dashboard when service use is likely to be adversely affected. Adobe also maintains a Status Health Dashboard for Adobe Creative Cloud for enterprise.

Patch Management

AWS maintains responsibility for patching systems that support the delivery of AWS services, such as the hypervisor and networking services. Adobe is responsible for patching its guest operating systems (OS), software, and applications running in AWS. When patches are required, Adobe supplies a new, pre-hardened instance of the OS and application rather than an actual patch.

Secure Management

Adobe uses Secure Shell (SSH) and Secure Sockets Layer (SSL) for management connections to manage the hosting infrastructure.

AWS Physical and Environmental Controls

AWS physical and environmental controls are specifically outlined in a SOC1-Type 2 report. The following section outlines some of the security measures and controls in place at AWS data centers around the world. For more detailed information about AWS security, please consult the AWS: Overview of Security Processes white paper or the Amazon security website.

Physical Facility Security

AWS data centers utilize industry standard architectural and engineering approaches. AWS data centers are housed in nondescript facilities and Amazon controls physical access both at the perimeter and at building ingress points using professional security staff, video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication (2FA) a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS 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, their access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Fire Suppression

AWS installs automatic fire detection and suppression equipment in all AWS data centers. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Controlled Environment

AWS employs a climate control system to maintain a constant operating temperature for servers and other hardware, preventing overheating and reducing the possibility of service outages. AWS data centers maintain atmospheric conditions at optimal levels. AWS personnel and systems monitor and control both temperature and humidity at appropriate levels.

Backup Power

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Video Surveillance

Professional security staff strictly controls physical access both at the perimeter and at building ingress points for AWS data centers using video surveillance, intrusion detection systems, and other electronicmeans.

Disaster Recovery

AWS data centers include a high level of availability and tolerate system or hardware failures with minimal impact. Housed in clusters in various global regions, all data centers remain online 24/7/365 to serve customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area.

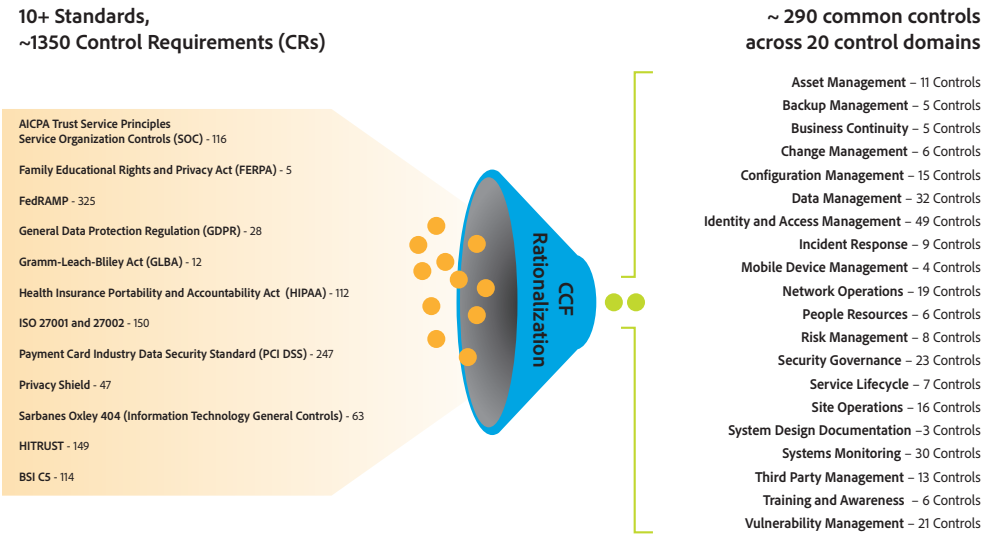
Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. You can find more information about AWS disaster recovery protocols on the Amazon Security website.

Adobe Common Controls Framework

To protect from the software layer down, Adobe uses the Adobe Secure Product Lifecycle (SPLC), which is described in a following section. To protect from the physical layer up, Adobe implements a foundational framework of security processes and controls to protect the company's infrastructure,

applications, and services that help Adobe comply with many industry-accepted best practices, standards, and certifications.

In creating the Adobe Common Controls Framework (CCF), Adobe analyzed the criteria for the most common security certifications and found several overlaps. After analyzing more than 1,000 requirements from relevant cloud security frameworks and standards, Adobe rationalized these requirements down to approximately 200 Adobe-specific controls needed to address the expectations of Adobe stakeholders and customers.

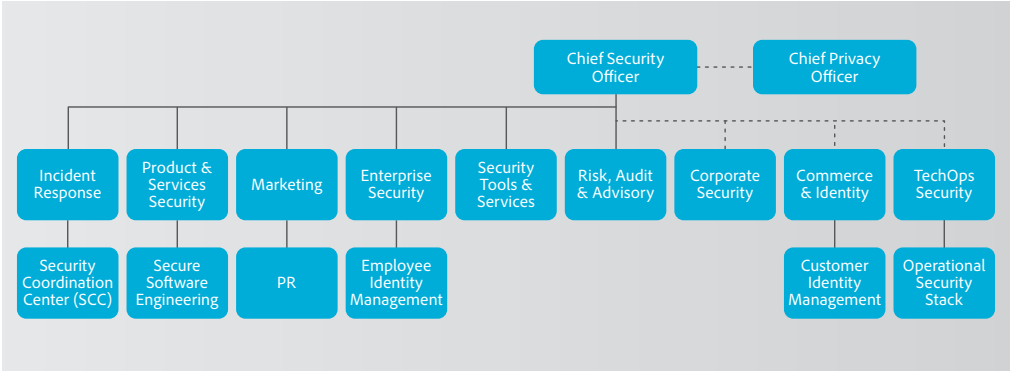


The Adobe Common Controls Framework (CCF)

Adobe Security Organization

As part of our commitment to the security of our products and services, Adobe coordinates all security efforts under the Chief Security Officer (CSO). The office of the CSO coordinates all product and service security initiatives and the implementation of the Adobe SPLC.

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security specialists who serve as consultants to key Adobe product and operations teams, including the Creative Cloud for enterprise team. ASSET researchers work with individual Adobe product and operations teams to strive to achieve the right level of security for products and services and advise these teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.



Adobe security organization

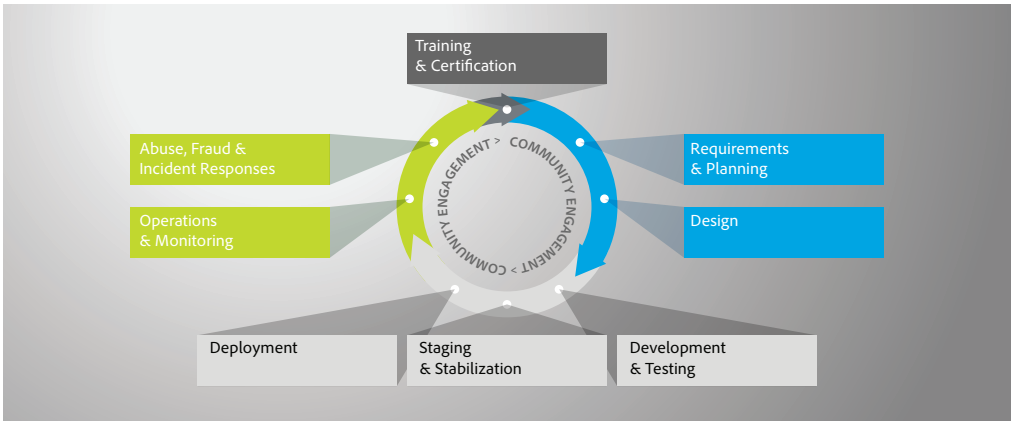
Adobe Secure Product Development

As with other key Adobe product and service organizations, the Creative Cloud organization employs the SPLC process. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment. ASSET security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

Adobe Secure Product Lifecycle

The Adobe SPLC activities include some or all of the following recommended practices, processes, and tools, depending on the specific Creative Cloud for enterprise service:

- Security training and certification for product teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis
- Service roadmaps, security tools, and testing methods that guide the Creative Cloud security team to help address the Open Web Application Security Project (OWASP) top ten most critical web application security flaws and CWE/SANS top 25 most dangerous software errors
- Security architecture review and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User Generated Content validation
- Dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials



Adobe Secure Product Lifecycle (SPLC)

Adobe Security Training

Adobe Software Security Certification Program

As part of the Adobe SPLC, Adobe conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services. Employees participating in the Adobe Software Security Certification Program attain different certification levels by completing security projects.

Various teams within the Creative Cloud organization participate in additional security training and workshops to increase the awareness of how security affects their specific roles within the organization and the company in general. For more information, please see the Adobe Security Culture white paper.

Adobe Risk and Vulnerability Management

Adobe strives to ensure that our risk and vulnerability management, incident response, mitigation, and resolution process is nimble and accurate. We continuously monitor the threat landscape, share knowledge with security experts around the world, swiftly resolve incidents when they occur, and feed this information back to our development teams to help achieve the highest levels of security for all Adobe products and services.

Business Continuity and Disaster Recovery

Adobe supports business continuity through the implementation and use of a fully supported Business Continuity and Disaster Recovery (BCDR) program. The Adobe BCDR program is managed by the Technology Governance, Risk, and Compliance (TechGRC) team in conjunction with the Office of the Chief Security Officer (CSO). The program's purpose is to ensure the safety of personnel, prepare Adobe to respond to business disruptions in a safe and timely manner and to facilitate the efficient restoration of critical business functions (CBF).

Applicable product and service teams at Adobe are required to integrate with this corporately sponsored and governed process to mitigate the risk of an unplanned continuity event. Adobe's BCDR program is supported by governing documentation, which is reviewed and updated annually, that covers business continuity, disaster recovery, BCDR testing, business impact analysis, and data backup and restoration processes.

Penetration Testing

Adobe approves and engages with leading third-party security firms to perform penetration testing that can uncover potential security vulnerabilities and improve the overall security of Adobe products and services. Upon receipt of the report provided by the third party, Adobe documents these vulnerabilities, evaluates severity and priority, and then creates a mitigation strategy or remediation plan.

Internally, the Adobe Creative Cloud for enterprise security team performs a risk assessment of the Creative Cloud for enterprise code prior to every release. Conducted by highly trained security staff trusted with securing the network topology and infrastructure, the security reviews look for insecure network setup issues across firewalls, load balancers, and server hardware, as well as for application-level vulnerabilities. The security touchpoints include exercises such as threat modeling coupled with vulnerability scanning as well as dynamic analysis of the application. The Creative Cloud for enterprise security team partners with the technical operations and development leads to help ensure all high-risk vulnerabilities are mitigated prior to each release.

Penetration tests are conducted at least annually or after every major release. Vulnerability scans are performed monthly while web and database scans are performed quarterly.

Incident Response and Notification

New vulnerabilities and threats evolve each day and Adobe strives to respond to mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including US-CERT, Bugtraq, and SANS, Adobe also subscribes to the latest security alert lists issued by major security vendors.

For more detail on Adobe's incident response and notification process, please go here.

Forensic Analysis

For incident investigations, the Creative Cloud team for enterprise adheres to the Adobe forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody recording.

Adobe Corporate Locations

Adobe maintains offices around the world and implements the following processes and procedures company-wide to protect the company against security threats.

Physical Security

Every Adobe corporate office location employs on-site guards to protect the premises 24x7. Adobe employees carry a key card ID badge for building access. Visitors must enter through the front entrance, sign in and out with the receptionist, display a temporary visitor ID badge, and be accompanied by an employee. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked in environmentally controlled server rooms accessible only by appropriate, authorized staff members at all times.

Virus Protection

Adobe scans all inbound and outbound corporate email for known malware threats, implementing anti-malware protection mechanisms for all systems and employee assets (e.g., laptops) commonly affected by malware (e.g., Windows servers). Anti-malware protection involves the following:

- Scanning signatures are updated daily
- Scan engine version is updated to stay current with vendor releases
- Full system scans are run weekly
- Event logs and alerts are generated
- Issues identified from scanning results are available to authorized parties or groups
- Real-time scanning is enabled
- Antivirus mechanisms cannot be disabled

Adobe Employees

Employee Access to Customer Data

Adobe maintains segmented development and production environments for Creative Cloud for enterprise, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems, and employees with no legitimate business purpose are restricted from accessing these systems. Access is given to employees using least privilege and access rights are reviewed quarterly.

Background Checks

Adobe obtains background check reports for employment purposes. The specific nature and scope of the report that Adobe typically seeks includes inquiries regarding educational background, work history, court records (including criminal conviction records), and references obtained from professional and personal associates, each as permitted by applicable law. These background check requirements apply to regular U.S. new-hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background check requirements through the applicable temporary agency, in compliance with Adobe's background screen guidelines. Outside the U.S., Adobe conducts background checks on certain new employees in accordance with Adobe's background check policy and applicable local laws.

Employee Termination

When an employee leaves Adobe, the employee's manager submits an "exiting worker" form. Once approved, Adobe People Resources initiates an email workflow to inform relevant stakeholders to take specific actions leading up to the employee's last day. If Adobe terminates an employee, Adobe People Resources sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination. Adobe Corporate Security then schedules the following actions to

help ensure that, upon conclusion of the employee's final day of employment, he or she can no longer access Adobe confidential files or offices:

- Email access removal
- Remote VPN access removal
- Office and datacenter badge invalidation
- Network access termination

Facility Security

Every Adobe corporate office location employs on-site guards to protect the premises 24x7. Adobe employees carry a key card ID badge for building access. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary Visitor ID badge and are accompanied by an employee. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environment-controlled server rooms accessible only by appropriate, authorized staff members.

Virus Protection

Adobe scans all inbound and outbound corporate email for known malware threats.

Customer Data Confidentiality

Adobe always treats customer data as confidential. Adobe does not use or share the information collected on behalf of a customer except as may be allowed in a contract with that customer and as set forth in the Adobe Terms of Use and the Adobe Privacy Policy.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of the Adobe Creative Cloud for enterprise solution and your confidential data. At Adobe, we take the security of your digital experience very seriously and we continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the secure our customers' data.

For more information, please visit: http://www.adobe.com/security

Adobe

Adobe
345 Park Avenue
San Jose, CA 95110-2704
USA
trust.adobe.com