

# Adobe® Connect Security



## Table of Contents

- 1 Overview
- 1 About Adobe Connect
- 1 Adobe Connect Solution Components
- 2 Adobe Connect Server Architecture
- 3 Adobe Connect Data Flow
- 5 Adobe Connect Security Architecture
- 6 User Authentication
- 6 Adobe Connect Hosted Multi-tenant Data Centers
- 7 Adobe Connect Hosted Multi-tenant Core Operational Security
- 9 Adobe Connect Hosted Multi-tenant Physical and Environmental Controls
- 13 Adobe Risk & Vulnerability Management
- 15 Adobe Corporate Security
- 16 Adobe Corporate Locations
- 17 Adobe Connect Compliance
- 18 Customer Data Confidentiality
- 19 Conclusion

## Overview

At Adobe, we take the security of your digital experiences 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 security best practices and trends and continually build security into the products and services we offer.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to bolster the security of your Adobe® Connect Hosted and Adobe Connect Managed Services experience and your data.

## About Adobe Connect

Adobe Connect is a secure web conferencing platform that offers immersive online meeting experiences for collaboration, virtual classrooms, and large-scale webinars. Powering end-to-end, mission-critical web conferencing solutions on virtually any device, Adobe Connect enables organizations to fundamentally improve productivity. Adobe Connect is available in two common deployment options:

**Adobe Connect Hosted Multi-tenant**, which uses a combination of Adobe and co-located infrastructure in a shared cloud deployment; and

**Adobe Connect Managed Services**, which uses the Amazon Web Services (AWS) cloud infrastructure in a private cloud deployment. Each ACMS customer has private images provisioned for the Adobe Connect application, database and storage.

On-premise deployment of Adobe Connect is also available.

## Adobe Connect Solution Components

Adobe Connect is comprised by two primary components: the Adobe Connect application suite and the Adobe Connect Server. All deployment options require both components, with the difference being the location of the Adobe Connect Server (hosted, managed service, or on-premise).

### Adobe Connect Application Suite

Adobe Connect includes a suite of five web-based software solutions:

**Adobe Connect Meeting**—Create, manage, and conduct online meetings, webinars, and virtual classrooms with polling, screen sharing, chat, live PowerPoint viewing and annotation, webcam and on-demand video, moderated Q&A, and more.

**Adobe Connect Training**—Create, manage, deploy, and track eLearning courses and curricula, complete with enrollment, assessments, surveys, learner management, and reporting.

**Adobe Connect Events**—Manage the full lifecycle of large- and small-scale events, such as email notification, event catalogs, registration management, reporting, and analytics.

**Adobe Presenter**—Rapidly create eLearning content and high-quality, multimedia, and on-demand presentations that can include narration, quizzes, and video.

**Adobe Connect Central**—Manage account-related information and content and use Adobe Connect Central to create meetings, manage presentations, create curriculums and events, view and download reports, and more.

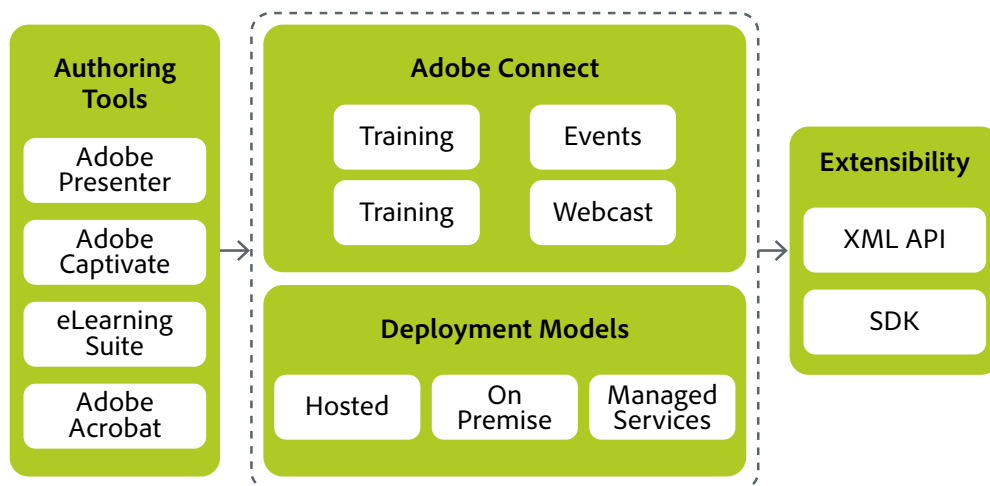


Figure 1: Adobe Connect Product Architecture

## Adobe Connect Server

Adobe Connect Server is an open platform server that delivers enterprise-class scalability with support for clustered environments and provides the reliability and redundancy to seamlessly support thousands of concurrent users.

In addition to the five (5) Adobe Connect software solutions, you can also publish training content and multimedia presentations directly to Adobe Connect Server from Adobe Captivate®. What's more, since Adobe Connect Server is an open platform, you can extend and integrate it with other, non-Adobe systems through a comprehensive set of APIs and a software development kit (SDK).

## Adobe Connect Server Architecture

As a multi-tier server, Adobe Connect Server separates logical functions across independent processes.

### Web Server

The application layer of Adobe Connect Server is built on J2EE using Apache Tomcat. Apache HTTP Server provides the web server functionality. The web server contains and executes all the business logic necessary for delivering content to users.

### Application Server

The Adobe Connect Server application server manages users, groups, on-demand content, and client sessions, among other tasks. Some of the application server's specific duties include access control, security, compliance, quotas, and licensing, as well as auditing and management functions, such as clustering, failover, and replication. It also transcodes media, such as Microsoft PowerPoint and Adobe PDF, to a format that allows viewing without the original application.

### Streaming Communication Server

Adobe Connect Server includes an embedded instance of Adobe Media Server that acts as the meeting server. This component handles all the real-time streaming of audio and video, synchronization of data, and delivery of rich media content. Adobe Media Server also plays a vital role in reducing server load and latency by caching frequently accessed streams and shared data.

Adobe Media Server uses the Real-Time Messaging Protocol (RTMP) but can be configured to use Secure Sockets Layer (SSL) for increased data security.

## Database

The Adobe Connect Server database persistently stores transactional and application metadata, including user, group, content, and reporting information. Adobe Connect Server can use either the embedded database engine (Microsoft SQL Server Express) or the full version of Microsoft SQL Server. Check the Adobe Connect system requirements for the most up-to-date information.

The embedded database engine must be installed on the same computer as Adobe Connect Server but is not recommended for production. When deploying Adobe Connect Server in a cluster, you must use the full version of Microsoft SQL Server and it cannot be installed on the same computer as Adobe Connect Server. Standard cluster and hot-swap configurations for Microsoft SQL Server are supported for scalability and failover.

## HTML Authoring/Publishing

Adobe Connect Server uses Adobe CQ, a web content management system, for creating and managing HTML-based templates used for event email notifications, landing pages, and user self-registration. It provides the ability to author and subsequently publish web pages.

Adobe CQ requires at least one author and one publish instance within the Adobe Connect Server deployment when the Adobe Connect Events module is enabled. All the web-page authoring-related work is done in the Adobe CQ author instance and replicated in the publish instance. The publish instance is the read-only view of the web pages that have been authored in the AdobeCQ author instance. Multiple Adobe CQ author and publish instances can be configured within a server cluster to provide increased scalability and failover.

## Analytics

Adobe Connect provides limited reporting functionality. Optionally, Adobe Analytics can be used with either Adobe Connect Hosted or Adobe Connect Managed Service to provide more robust reporting and analytics for Adobe Connect events. These reports track viewing of landing pages; response to registration questions; attendance at meetings, webinars, or training; and even participation in polls, Q&A, and file download activity during meetings.

## Media Transcoding

Adobe Connect Server provides a number of file conversion utilities to automatically convert popular document formats into high-quality files to display in the meeting room. It converts PowerPoint files (e.g., .ppt and .pptx) into small, vector-based files, providing the highest-quality, resolution-independent display for all participants. The conversion also accurately reproduces hyperlinks and virtually all of the original animations contained within each slide. Each Adobe Connect client pre-caches the individual slides when they are loaded into a meeting room, using minimal bandwidth to maintain synchronization across all users and ensuring the lowest latency transitions. Adobe Connect Server displays animations exactly as they appear in the original slides and keeps all hyperlinks clickable. Other supported file formats, such as PDF, are similarly converted.

## Adobe Connect Data Flow

Adobe Connect uses the HTTP, HTTPS, RTMP, and RTMPS protocols. RTMP is optimized to deliver real-time, rich media streams. RTMPS is the secure implementation of RTMP.

The connection paths for unencrypted and encrypted communications between Adobe Connect clients and Adobe Connect Server differ.

## Unencrypted Connections

Adobe Connect unencrypted connections use HTTP and RTMP and follow the paths described in the table below. By default data in transit is encrypted. The numbers in the table correspond to the numbers in Figure 3, below.

1. The Adobe Connect client requests a meeting or content URL over HTTP:80.
2. The web server responds and transfers the content or provides the Adobe Connect client with information to connect to the meeting.
3. The Adobe Connect client requests a connection to the meeting over RTMP:1935.
4. Adobe Media Server responds and opens a persistent connection for Adobe Connect streaming traffic.
- 3a. The Adobe Connect client requests a connection to the meeting but can only connect over RTMPT:443.
- 4a. Adobe Media Server responds and opens a tunneled connection for Adobe Connect streaming traffic.

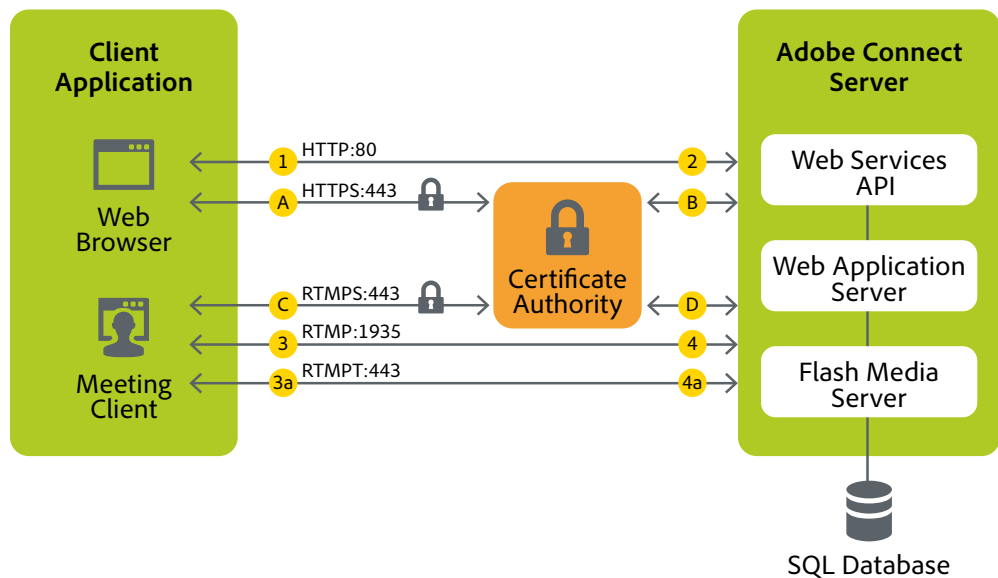


Figure 2: Adobe Connect data flow

## Encrypted Connections

Adobe Connect encrypted connections use HTTPS and RTMPS and follow the paths described in the table below. The letters in the table correspond to the letters in Figure 3, above.

- A. The Adobe Connect client requests a meeting or content URL over a secure connection on HTTPS:443.
- B. The web server responds and transfers the content over a secure connection or provides the Adobe Connect client with information to securely connect to the meeting.
- C. The Adobe Connect client requests a secure connection to Adobe Media Server over RTMPS:443.
- D. Adobe Media Server responds and opens a secure, persistent connection for Adobe Connect streaming traffic.

## Data Encryption

As information flows between Adobe Connect client applications and Adobe Connect Server, advanced industry-standard data encryption methods safeguard the confidential information contained within

**Adobe Connect Hosted**—Provides encryption in transit with a single key for all customers. TLS 1.0, 1.1, and 1.2 are used. Passwords are encrypted in the database, but no other encryption at-rest is used.

**Adobe Connect Managed Services**—Provides both encryption in-transit as well as encryption at-rest. The customer can determine the version of TLS best-suited to their needs. All data is encrypted using AES-256.

## Adobe Connect Security Architecture

### Administrator features

Customers control users, content, access, and features through the administration controls of Adobe Connect. Customers retain ownership of their content and data. The compliance and control settings are account-wide settings that broadly consist of the following:

- **Disable undesired functionality**—Administrators can turn off certain functional modules as needed
- **Disable screen sharing**—Administrators can prevent sharing of desktop, windows, or applications. They can also restrict screen sharing to specific applications or prevent specified applications from being shared.
- **Record and retain communications for auditing purposes**—Administrators can force recordings for all meetings, log all chat messages in files, and show a notice or disclaimer to all participants. Recordings can also be disabled for all meetings.
- **Control access to meetings**—Administrators and hosts can completely disable guest access so that guests can no longer request entry. Hosts can also automatically deny access to specific users and groups. Unlike the previous two categories, meeting access control settings are enforced on a per-meeting basis, not for the entire system or hosted account.

An administrator or limited administrator can also customize the permissions list for a file or folder. These permissions include:

- **Manage**—Users or groups with Manage permission for a folder or file can view, delete, move, and edit the file or folder, view reports for files in that folder, set permissions for the file or folder, and create new folders. However, they cannot publish to that folder.
- **Denied**—Users or groups with a Denied permission setting for a folder or file cannot view, publish, or manage this folder or file.
- **Publish**—Users or groups with a Publish permission setting for a folder or presentation can publish, update, and view presentations, as well as view reports for files in that folder. However, these users must also be members of the Built-in Author group, as well as have Publish permission, to publish content to this folder.
- **View**—Users or groups with a View permission setting for a folder or file can view any content in the folder or an individual file.

Administrators can also give meeting hosts the ability to mandate a passcode for Adobe Connect sessions. If a user incorrectly enters a password five (5) times, the account is locked out for five (5) minutes and the user is notified by email that the account has been temporarily suspended. Users can reset their passwords to create their own passwords based on the password policy set by the account administrator. Administrators can mandate a password change or set a temporary password for any user. Meeting hosts can lock out new participants, expel current participants, disable remote control, and disable the ability of participants to change their displayed name.

## User Authentication

Adobe Connect uses standard access control lists with password policy options and Transport Layer Security (TLS) encryption to secure access, content, and data. Passwords can be set to expire as well as require certain characters. Administrators can mandate that a password include a number, a capital letter, and/or a special character as well as require passwords to be of a minimum and/or a maximum length. In addition, old passwords can be tracked to prohibit reuse. Administrators can configure the number of old passwords that can be tracked.

Adobe Connect allows administrators to provision user accounts in several ways:

1. Manual provisioning through the use of a .csv file; or
2. Using the Adobe Connect Events module; or
3. Using the webservice API; or
4. For Adobe Connect Managed Services, using LDAP/AD synchronization.

Authentication takes place on the login screen of the Adobe Connect client or through the webservice API. For Adobe Connect Managed Services, administrators can also enable HTTP header authentication as well as LDAP/AD authentication.

## Single Sign-On

Adobe Connect does not provide out-of-the box-support for either Security Assertion Markup Language (SAML) or Open Authorization (OAuth) at this time. However, several partners have developed add-on solutions for single sign-on (SSO) for all deployment models. These solutions take advantage of the open and published webservice API, HTTP header authentication (Adobe Connect Managed Services and on-premise deployments only) and login page customization for the purpose of redirection (Adobe Connect Managed Services and on-premise deployments only). LDAP synchronization and authentication is available on Adobe Connect Managed Services and on-premise deployments only.

Adobe Connect Central (web application) handles application and service entitlement. More information is available at: <https://helpx.adobe.com/adobe-connect/using/setting-permissions-library-files-folders.html>

## Adobe Connect Hosted Multi-tenant Data Centers

Adobe Connect Hosted is hosted on Adobe servers four (4) locations around the world in a shared cloud (multi-tenant) deployment. These data centers are located in Hillsboro, Oregon; Dallas, Texas; London, England; and Sydney, Australia.

Adobe generally hosts the customer's deployment in a data center located in the customer's corresponding region. For Adobe Connect Hosted, multiple customer deployments reside on the same cluster of servers.



Figure 3: Adobe Connect Hosted Multi-tenant data center locations

## Adobe Connect Hosted Multi-tenant Core Operational Security

Adobe understands the importance of securing the data collection, data content serving, and reporting activities over the Adobe Connect network, which is comprised by Adobe-managed infrastructure. To this end, the network architecture implements industry best practices for security design, including segmentation of development and production environments, DMZ segments, hardened bastion hosts, and unique authentication.

### Segregating Client Data

Adobe Connect Hosted relies on application permissions to isolate one customer from another. The only access to these servers and databases is via secure access using the Adobe Connect application. All other access to the application and data servers is made only by authorized Adobe personnel and is conducted via encrypted channels over secure management connections. Adobe also separates our testing environments from our production environments to avoid use of customer data in testing environments.

### Secure Management

Adobe deploys dedicated network connections from our corporate offices to our data center facilities in order to enable secure management of the Adobe Connect servers. All management connections to the servers occur over encrypted Secure Shell (SSH), Secure Sockets Layer (SSL), or Virtual Private Network (VPN) channels and remote access always requires two-factor authentication. Unless the connection originates from a list of trusted IP addresses, Adobe does not allow management access from the Internet.

### Firewalls and Load Balancers

The firewalls implemented on the Adobe Connect network deny all Internet connections except those to allowed ports, Port 80 for HTTP and Port 443 for HTTPS. The firewalls also perform Network Address Translation (NAT). NAT masks the true IP address of a server from the client connecting to it. The load balancers proxy incoming HTTP/HTTPS connections and also distribute requests that enable the network to handle momentary load spikes without service disruption. Adobe implements fully redundant firewalls and load balancers, reducing the possibility that a single device failure can disrupt the flow of traffic.

## **Non-routable, Private Addressing**

Adobe maintains all servers containing customer data on servers with non-routable IP addresses (RFC 1918). These private addresses, combined with the Adobe Connect firewalls and NAT, help prevent an individual server on the network from being directly addressed from the Internet, greatly reducing the potential vectors of attack.

## **Intrusion Detection**

Both NIDS and HIDS are integrated into our centralized SIEM and are continuously monitored by the Digital Marketing Information Security Team. The security team follows up on intrusion notifications by validating the alert and inspecting the targeted platform for any sign of compromise. Adobe regularly updates all sensors and monitors them for proper operation.

## **Service Monitoring**

Adobe monitors all of our servers, routers, switches, load balancers, and other critical network equipment on the Adobe Connect network 24 hours a day, 7 days a week, 365 days a year (24x7x365). The Adobe Network Operations Center (NOC) receives notifications from the various monitoring systems and will immediately attempt to fix an issue or escalate the issue to the appropriate Adobe personnel. Additionally, Adobe contracts with multiple third parties to perform external monitoring.

## **Data Backups**

Adobe backs up customer content and data for Adobe Connect on a weekly basis, with daily differentials for disaster recovery purposes. These backups are also replicated to a hot failover site that is geographically removed from the primary data center. Adobe tests backups quarterly. The combination of backup procedures provides quick recovery from short-term backup as well as off-site protection of data.

## **Change Management**

Adobe maintains a formal change management process that includes documentation of impact testing prior to deployment to production and requires management sign-off by appropriate parties for all changes to system components as well as back-out procedures for all changes.

Adobe Connects release schedule is typically one major release every 12 to 18 months, with a minor release following the major release by six months and patches as needed.

While most maintenance does not require downtime, when it does, a typical downtime maintenance window will fall on a Friday evening from 8pm-midnight Pacific Time. Adobe Connect maintenance windows that include downtime are scheduled on an as-needed basis and are typically used for more involved maintenance (major releases) that will require part of the system to be unavailable for a period of time. There is no option for delaying or scheduling maintenance on the hosted service. All patches, updates, and hotfixes are tested prior to deployment. Prior to deployment, manager approval is required.

## **Patch Management**

In order to automate patch distribution to host computers within the Adobe Connect organization, Adobe uses internal patch and package repositories as well as industry-standard patch and configuration management. Depending on the role of the host and the criticality of pending patches, Adobe distributes patches to hosts at deployment and on a regular patch schedule. If required, Adobe releases and deploys emergency patch releases on short notice.

## **Access Controls**

Only authorized users within the Adobe intranet or remote users who have completed the multi-factor authentication process to create a VPN connection can access administrative tools. In addition, Adobe logs all server connections for auditing.



## Logging

In order to protect against unauthorized access and modification, Adobe captures network logs, OS-related logs, and intrusion detections. Sufficient storage capacity for logs is identified, periodically reviewed, and, as needed, expanded to help ensure that log storage is not exceeded. Systems generating logs are hardened and access to logs and logging software is restricted to authorized Adobe Digital Marketing Information Security Team personnel.

## Adobe Connect Hosted Multi-tenant Physical and Environmental Controls

The below description of data center physical and environmental access controls includes controls that are common to all Adobe data center locations. Some data centers may have additional controls to supplement those described in this document.

### Physical Facility Security

Adobe physically secures all hardware in Adobe-owned or -leased hosting facilities against unauthorized access. All facilities that contain production servers for Adobe Connect include dedicated, 24-hour on-site security personnel and require these individuals to have valid credentials to enter the facility. Adobe requires PIN or badge credentials—and, in some cases, both—for authorized access to data centers. Only individuals on the approved access list can enter the facility. Some facilities include the use of man-traps, which prevent unauthorized individuals from tailgating authorized individuals into the facility.

### Fire Suppression

All data center facilities must employ an air-sampling, fast-response smoke detector system that alerts facility personnel at the first sign of a fire. In addition, each facility must install a pre-action, dry-pipe sprinkler system with double interlock to ensure no water is released into a server area without the activation of a smoke detector and the presence of heat.

### Controlled Environment

Every data center facility must include an environmentally controlled environment, including temperature humidity control and fluid detection. Adobe requires a completely redundant heating, ventilation, and air conditioning (HVAC) system and 24x7x365 facility teams to handle environmental issues promptly that might arise. If the environmental parameters move outside those defined by Adobe, environmental monitors alert both Adobe and the facility's Network Operations Center (NOC).

### Video Surveillance

All facilities that contain product servers for Adobe Connect must provide video surveillance to monitor entry and exit point access, at a minimum. Adobe asks that data center facilities also monitor physical access to equipment. Adobe may review video logs when issues or concerns arise in order to determine access.

### Backup Power

Multiple power feeds from independent power distribution units help to ensure continuous power delivery at every Adobe-owned or Adobe-leased data center facility. Adobe also requires automatic transition from primary to backup power and that this transition occurs without service interruption. Adobe requires each data center facility to provide redundancy at every level, including generators and diesel fuel contracts. Additionally, each facility must conduct regular testing of its generators under load to ensure availability of equipment.

## Disaster Recovery

In the event that one of our data collection environments is unavailable due to an event, whether a problem at the facility, a local situation, or a regional disaster, Adobe follows the process described here to allow for continuation of data collection and to ensure an effective and accurate recovery:

### *Failover Process*

When an event is determined to result in long-term service disruption, Adobe will reconfigure DNS to send requests to a secondary data center location not affected by the disruption.

DNS record TTL (time to live) is set to allow this switch to the secondary location to happen quickly. While product components are in a failover mode, customers are notified of the ongoing situation with regular status updates. If the disaster at the primary server locations is serious enough to have destroyed or make any needed historical data there unavailable, Adobe will restore that data from backups stored at off-site locations.

### *Recovery Process*

When the primary data collection location is available and stable again, the failover process will be reversed. All traffic collected at the secondary location will be merged with data in the primary location, DNS records will be restored, and held requests will be processed sequentially. Time required to recover historical data from off site may take up to an additional ten (10) days.

### Adobe Connect Managed Services Core Operational Security

Adobe Connect Managed Services is hosted on Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3), in Amazon's U.S. East (Northern Virginia), U.S. West (San Jose, California), EU West (Dublin, Ireland), and Asia/Pacific Southeast (Singapore) regions for commercial customers. For government customers, Adobe Connect Managed Services is hosted in AWS' U.S. Government West (Hillsboro, Oregon) data center. Amazon EC2 is a web service that provides resizable compute capacity in the cloud, making web-scale computing easier. Amazon S3 is a highly redundant data storage infrastructure for storing and retrieving any amount of data, at any time, from anywhere.



Figure 4: Adobe Connect Managed Service data center locations

Each of Amazon's cloud regions is composed of two or more availability zones, which are in turn composed of one or more data centers. Each availability zone is designed to be both physically (separate geographical dependencies, power sources, cooling, etc.) and logically (Internet peering connections, control systems, etc.) separate from the others. Adobe Connect Managed Services is designed to handle disaster recovery between availability zones but is not configured to fail between cloud regions.

The AWS platform provides services in accordance with industry-standard practices and undergoes regular industry-recognized certifications and audits. You can find more detailed information about AWS and Amazon's security controls on the [AWS security site](#).

## **Operational Responsibilities of AWS and Adobe**

AWS operates, manages, and controls the components from the hypervisor virtualization layer down to the physical security of the facilities in which Adobe Connect operates. In turn, Adobe assumes responsibility 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 AWS infrastructure includes facilities, network, and hardware, as well as the operational software (e.g., host OS, virtualization software, etc.) that supports the provisioning and use of these resources. Amazon designs and manages AWS 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 AWS infrastructure.

## **Geographic Location of Customer Data on AWS Network**

The following information is from the AWS: Overview of Security Processes White paper. For more detailed information about AWS security, please consult the [AWS white paper](#).

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.

## **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 the 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. Amazon Information Security approves all ACL policies and automatically pushes them to each managed interface using AWS's ACL-Manage tool, helping to 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](#) on the Amazon website.

## **Intrusion Detection**

Adobe actively monitors Adobe Connect using industry-standard Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

## **Logging**

Adobe conducts server-side logging of Adobe Connect customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs only store Adobe 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 Connect Managed Services provides an automatic backup service as a part of the standard product offering. This—together with the master image or AMI of the software executables taken before transition to production and after each upgrade to the system, both of which are disseminated securely across multiple AWS availability zones—allows Adobe to quickly recover from a wide variety of failure scenarios. See the following for additional detail regarding the Adobe Connect Managed Services environment: <ftp://ftp.connectusers.com/connect/Managed%20Service%20Backup%20%26%20Disaster%20Recovery%20Brochure.pdf>

Adobe stores all Adobe Connect data in Amazon S3, which provides a storage infrastructure with high durability. To help provide 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. For more detailed information about AWS security, please consult the AWS: Overview of Security Processes white paper.

## **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 Connect.

Adobe Connect Managed Services follows a Change Approval Board (CAB) process for any and all changes that could impact customer experience. The CAB process focuses upon enforcing stability and availability, while permitting an agile response to emerging issues, and providing internal process transparency and accountability.

## **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.

## Adobe Risk & 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.

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

### 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.

When a significant announced vulnerability puts Adobe Connect at risk, the Adobe PSIRT (Product Security Incident Response Team) communicates the vulnerability to the appropriate teams within the Captivate organization to coordinate the mitigation effort.

For Adobe cloud-based services, including Adobe Connect, Adobe centralizes incident response, decision-making, and external monitoring in our Security Coordination Center (SCC), providing cross-functional consistency and fast resolution of issues.

When an incident occurs with an Adobe product or service, the SCC works with the involved Adobe product incident response and development teams to help identify, mitigate, and resolve the issue using the following proven process:

- Assess the status of the vulnerability
- Mitigate risk in production services
- Quarantine, investigate, and destroy compromised nodes (cloud-based services only)
- Develop a fix for the vulnerability
- Deploy the fix to contain the problem
- Monitor activity and confirm resolution

### Forensic Analysis

For incident investigations, the Adobe Connect team 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.

## **AWS Physical and Environmental Controls**

AWS physical and environmental controls are specifically outlined in a SOC 1, 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 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, his or her 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 electronic means.

### **Disaster Recovery**

AWS data centers include a high level of availability and tolerate system or hardware failures with minimal impact. Built 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 Corporate Security

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 Secure Product Lifecycle (SPLC).

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security experts who serve as consultants to key Adobe product and operations teams, including the Adobe Connect 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.

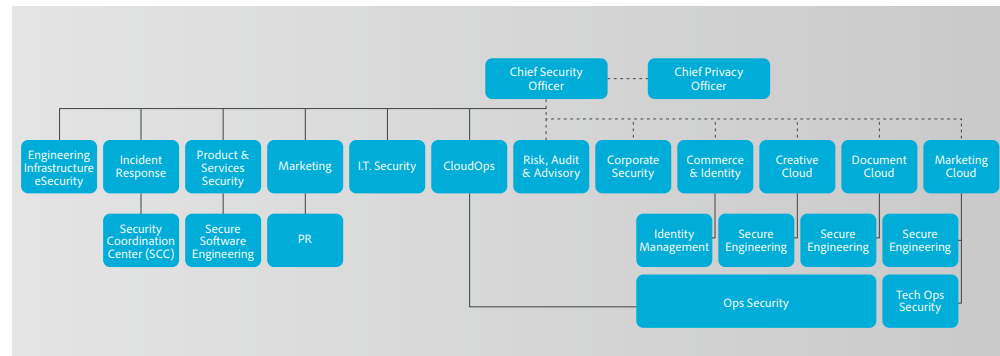


Figure 4: The Adobe Security Organization

## Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe Connect organization employs the Adobe Software Product Lifecycle (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, depending on the specific Connect component, some or all of the following recommended best practices, processes, and tools:

- 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 Adobe Connect security team to help address the Open Web Application Security Project (OWASP) Top 10 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
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials

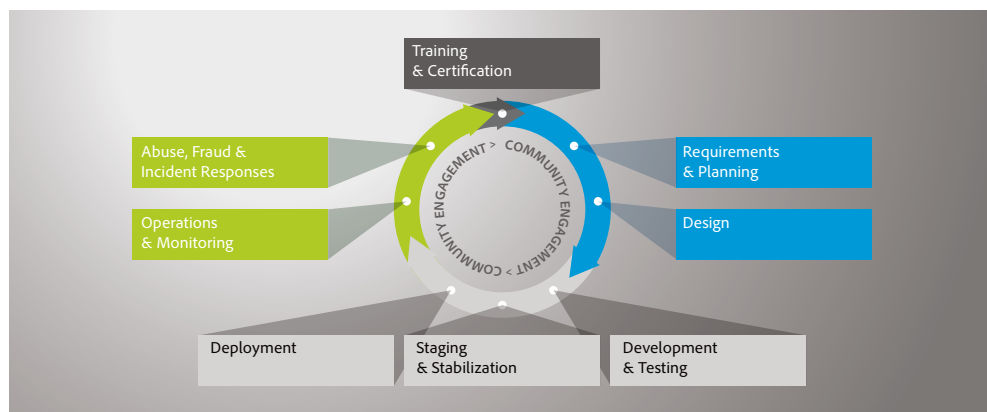


Figure 5: Adobe Secure Product Lifecycle (SPLC)

## 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.

The program has four levels, each designated by a colored 'belt': white, green, brown, and black. The white and green levels are achieved by completing computer-based training. The higher brown and black belt levels require completion of months- or year-long hands-on security projects. Employees attaining brown and black belts become security champions and experts within their product teams. Adobe updates training on a regular basis to reflect new threats and mitigations, as well as new controls and software languages.

Various teams within the Connect organization participate in additional security training and workshops to increase awareness of how security affects their specific roles within the organization and the company as a whole.

## 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 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.

### Adobe Employees

#### *Employee Access to Customer Data*

Adobe maintains segmented development and production environments for Connect, 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.



## 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. In the event that 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 to Adobe confidential files or offices:

- Email Access Removal
- Remote VPN Access Removal
- Office and Datacenter Badge Invalidation
- Network Access Termination

Upon request, managers may ask building security to escort the terminated employee from the Adobe office or building.

## Adobe Connect Compliance

The Adobe Common Controls Framework (CCF) is a set of security activities and compliance controls that are implemented within our product operations teams as well as in various parts of our infrastructure and application teams. In creating the CCF, Adobe analyzed the criteria for the most common security certifications for cloud-based businesses and rationalized the more than 1,000 requirements down to Adobe-specific controls that map to approximately a dozen industry standards.

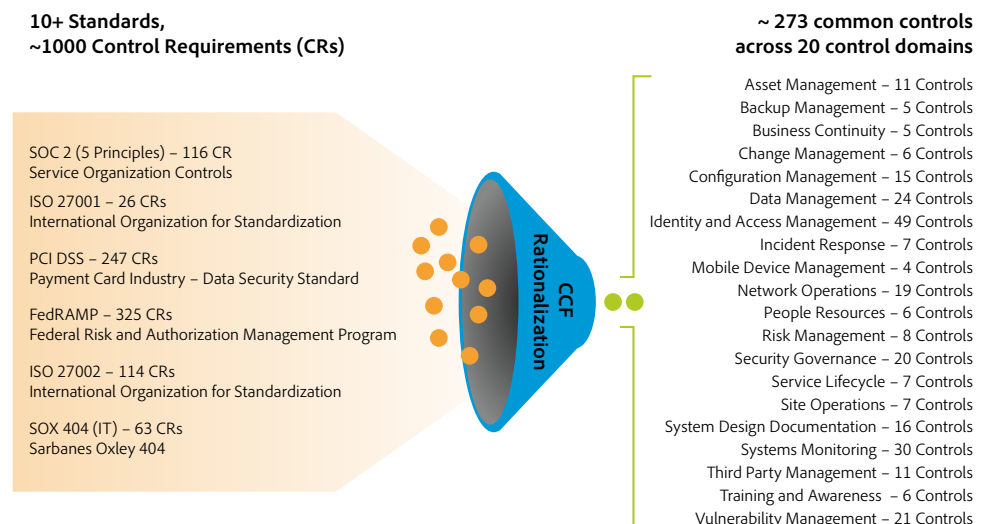


Figure 6: The Adobe Common Controls Framework (CCF)

## Current Regulations and Compliance for Adobe Connect Hosted

**SOC 2** is a set of security principles that define leading practice controls relevant to security, confidentiality, and privacy. Adobe Connect Hosted is SOC 2 – Type 2 (Security & Availability) compliant.

**ISO 27001** is a set of globally adopted standards that outline stringent security requirements and provide a systematic approach to managing the confidentiality, integrity, and availability of customer information. Adobe Connect Hosted is compliant with ISO 27001:2013.

**The Gramm-Leach-Bliley Act (GLBA)** requires that financial institutions safeguard their customers' personal data. Adobe Connect Hosted is "GLBA-ready," meaning that it enables our FSI customers to comply with the GLBA Act requirements for using service providers. Ultimately, the customer is responsible for ensuring their compliance with their legal obligations, that our solutions meet their compliance needs, and that they secure the solutions in an appropriate way.

## Current Regulations and Compliance for Adobe Connect Managed Service

**SOC 2** is a set of security principles that define leading practice controls relevant to security, confidentiality, and privacy. Adobe Connect Managed Services is SOC 2 – Type 2 (Security & Availability) compliant.

**ISO 27001** is a set of globally adopted standards that outline stringent security requirements and provide a systematic approach to managing the confidentiality, integrity, and availability of customer information. Adobe Connect Managed Services is compliant with ISO 27001:2013.

**The Gramm-Leach-Bliley Act (GLBA)** requires that financial institutions safeguard their customers' personal data. Adobe Connect Managed Services is GLBA-Ready, meaning that it enables our FSI customers to comply with the GLBA Act requirements for using service providers. Ultimately, the customer is responsible for ensuring their compliance with their legal obligations, that our solutions meet their compliance needs, and that they secure the solutions in an appropriate way.

**The Federal Risk and Authorization Management Program (FedRAMP)** is a collection of mandatory standards established by the U.S. Federal Government for security assessment and purchase approval for cloud solutions. Adobe Connect Managed Services is compliant with FedRAMP.

**The Health Insurance Portability and Accountability Act (HIPAA)** is legislation that governs the use of electronic medical records, and it includes provisions to protect the security and privacy of personally identifiable health-related data, called protected health information (PHI). Adobe Connect Managed Services is HIPAA-compliant, which means it can enable our enterprise customers to use our solutions in a way that they can meet their obligations under HIPAA regulations. Ultimately, the customer is responsible for ensuring their compliance with their legal obligations, that our solutions meet their compliance needs, and that they secure the solutions in an appropriate way.

**The U.S. Family Education Rights and Privacy Act (FERPA)** is designed to preserve the confidentiality of U.S. Student education records and directory information. Under FERPA guidelines, Adobe can contractually agree to act as a "school official" when it comes to handling regulated student data and therefore to enable our education customers to comply with FERPA requirements. Ultimately the customer is responsible for ensuring their compliance with their legal obligations, that our products meet their compliance needs, and that they secure the products in an appropriate way. Adobe Connect Managed Services is FERPA-Ready.

## Customer Data Confidentiality

Adobe 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](#). Adobe Systems Incorporated (our U.S. company) also adheres to the [European Union Safe Harbor Privacy Program](#).

## Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Connect 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 stay ahead of malicious activities and help ensure the secure our customers' data.

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



Adobe Systems Incorporated  
345 Park Avenue  
San Jose, CA 95110-2704  
USA  
[www.adobe.com](http://www.adobe.com)

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative. Further details on the Adobe solution, including SLAs, change approval processes, access control procedures, and disaster recovery processes are available.

[www.adobe.com](http://www.adobe.com)

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 06/2017 Adobe Systems Incorporated. All rights reserved. Printed in the USA.