Adobe® Connect™ hosted deployment

Meeting your most demanding security requirements and providing a secure foundation for building your solutions

Table of contents

1 Physical security
1 Network security
2 Meeting security
3 Data security
3 Software development and testing
3 Security reviews and certifications
3 Summary
3 For more information

Adobe Connect software provides a secure web conferencing platform for web meetings, eLearning, and webinars. It powers end-to-end, mission critical web conferencing solutions on virtually any device, enabling organizations from leading corporations to the U.S. Department of Defense (DoD) to fundamentally improve productivity. With its strong emphasis on security from the physical to the application level, Adobe Connect can meet your most demanding security requirements and provide a secure foundation for building your solutions. Adobe Connect is available as hosted, on-premise, and managed services deployments. This white paper focuses on the Adobe Connect hosted deployment, although it also references other deployment options for particular features.

Physical security

Adobe employs data centers across the globe that have world-class security measures, including but not limited to on-premise security guards, exterior security systems (cameras with recorders, vehicle blockades, bulletproof glass/walls, and unmarked buildings), biometric systems, and mantraps. Adobe monitors and records all areas of the data centers using closed circuit television (CCTV), and it controls all access points.

All data center visitors must present identification and sign in. During their visit, they are continually escorted by authorized staff. Adobe only provides data center access and information to those who have a legitimate business need for such privileges. When someone no longer has a business need for these privileges, his or her access is immediately revoked.

Adobe helps ensure the physical security and integrity of its physical assets. All old media is wiped out using industry standard technologies. Adobe also helps ensure other physical safeguards (backup power, HVAC, fire suppression, earthquake and flood protection) are provided.

Adobe routinely logs and audits all physical access to data centers. Equipment access logs are reviewed regularly. All security personnel undergo extensive background checks prior to being hired. After hiring, they must complete mandatory security training.

Network security

Application monitors are in place across all information systems. Alerts are configured for a large variety of error conditions and standard operating procedures are in place for responding to these alerts. Monitors are updated in response to observed issues, as well as with updates to Adobe Connect. Application, server, database, security, and other information system logging is consolidated for review by support and operations teams and is leveraged for advanced alerting.

All application and device logs are saved for 30 days and made available to authorized personnel only. Syslog is utilized to capture and retransmit any system messages—system messages with a severity code of warning or above are recorded by the Central Log Management System and stored locally. Events with a severity code higher than warning are acted upon promptly. A centralized internal time source via the Network Time Protocol (NTP) protocol is used to synchronize systems and provide accurate audit log time stamping. Device logs are regularly audited to help ensure there is no suspicious activity.

Firewalls are managed according the Adobe Connect Change Management Policy. The Change Management Policy, procedures, and system adhere to the following high-level requirements:

- All proposed changes are documented prior to deployment to the stage and production environments
- Scheduled change implementations do not conflict with Adobe business cycles, priorities, or IT blackout periods
- Appropriate risk assessment, management involvement, and approvals exist for all changes
- Adequate testing and verification are completed prior to release
- Audit trails are created and maintained for all service changes. Access follows the least privilege principle.

Multiple industry standard practices are used to mitigate distributed denial-of-service (DDoS) attacks, including deep packet analysis, traffic throttling, and packet black-holing. Defenses are in place against both internal and external attacks. Production environments are physically isolated by utilizing network access lists (ACLs), firewalls, virtual private network (VPN) tunnels, and separate physical servers. Hardening is at the server and network layers, and is implemented with the principle of least privilege to separate the various tiers.

Meeting security

You control users, content, access, and features through the administration controls of Adobe Connect. 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 and named pods to disable instance chat and displaying of attendee names.
- **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 customize the permissions list for a file or folder. These permissions are:

- **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.

Meetings use standard ACLs with password policy options and Secure Sockets Layer (SSL) encryption. You can set passwords to expire after a certain number of days. Password policy can require certain characters, including a number and/or a capital letter, and require a minimum length and/or a maximum length. Meeting hosts can mandate a passcode for meetings. Users can reset their passwords to create their own passwords. Administrators can also change passwords. Passwords are hashed using SHA-256 with 16 bytes salt.

Meeting hosts can lock out new participants, expel current participants, disable remote control, and disable the ability of participants to change their displayed name.

ACMS and the Adobe Connect on-premise deployment provide authentication support via LDAP, Active Directory, Public Key Infrastructure (PKI), OAuth 2.0, and Security Assertion Markup Language (SAML).

Data security

All data traffic is SSL enabled (HTTPS by default; RTMPS is optional; both 128-bit and 256-bit are supported). Data is isolated and restricted to respective users. The data is collected by the Adobe Connect server and is processed based on the features used. It remains in the data center where the account was provisioned until it is downloaded, moved, or deleted. Adobe has a Safe Harbor Privacy Policy; for more information, visit *www.adobe.com/privacy/safe-harbor.html*.

Software development and testing

Adobe Connect has robust security features. It adheres to the Adobe Secure Product Lifecycle (SPLC). For more information about SPLC, visit *www.adobe.com/security/splc*. Access to the source code is restricted. The testing organization regularly scans the source code. Security code reviews follow guidelines and best practices set by the Adobe Secure Software Engineering Team (ASSET). The Adobe Connect team works closely with the Adobe Product Security Incident Response team (PSIRT) to quickly address any reported product vulnerabilities. For more information about PSIRT, visit *www.adobe.com/security/psirt*.

There are distinct and separate environments for development, testing, staging, and production. Prior to making any change to a production system, the change is first applied and validated in a staging environment. Per Adobe change management policies, the change is only allowed to be applied to the production system if it is successfully validated in a staging environment. No sensitive data is used for testing purposes.

Security reviews and certifications

Adobe Connect uses the services of external independent InfoSec vendors for annual security evaluations. The findings are made public. For most recent security evaluation report, visit *wwwimages.adobe.com/www.adobe.com/content/dam/Adobe/en/products/adobeconnect/pdfs/security/Adobe_Connect9_Security_Assessment_Hosted.pdf.*

Adobe Connect is TRUSTe and Joint Interoperability Test Command (JITC) certified. The Adobe Connect hosted deployment is also Service Organization Controls 2 (SOC 2) compliant. SOC 2 replaces SAS 70; portions of a SOC 2 Report can address some aspects of Federal Information Security Management Act (FISMA), ISO27001, and Health Insurance Portability and Accountability Act (HIPAA) certifications. Adobe Connect Managed Services (ACMS) is fully HIPAA compliant.

Summary

You can confidently conduct meetings, eLearning, and webinars on the Adobe Connect highly secure web conferencing platform. The Adobe Connect robust set of security features and commitment to security gives you peace of mind and enables you to focus on collaborating effortlessly and productively.

For more information

Solution details: *www.adobe.com/products/adobeconnect.html*

Adobe

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

2/14