Adobe Experience Manager Screens Security Overview

Table of Contents

Adobe Security

At Adobe, we take the security of your digital experience very seriously. Security practices are deeply ingrained into our internal software development and operations processes and tools and are rigorously followed by our cross-functional teams to prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, security research institutions, and other industry organizations helps us keep up to date with the latest threats and vulnerabilities and we regularly incorporate advanced security techniques 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 signage solution based on the Adobe Experience Manager Screens application and your data. For more detailed information about security best practices when deploying and using Adobe Experience Manager (AEM) Screens, please refer to our documentation on best practices for developers and our recommended security checklist.

About Adobe Experience Manager Screens

AEM Screens is a secure digital signage solution that allows customers to publish dynamic and interactive digital experiences and interactions onto different types of digital screens to improve brand perception, impact in-store and in-venue demand, and influence purchase decisions.

Built on the solid foundation of AEM Sites, Adobe's market-leading web experience management solution, AEM Screens enables marketers and IT personnel to create and manage content on multiple digital screens within the framework of a comprehensive marketing platform. Existing content in AEM Sites can be quickly and easily leveraged to deliver a coherent and consistent customer experience on a variety of screens, providing a streamlined workflow that creates cost-effective and usable digital experiences.

Adobe Experience Manager Screens Solution Architecture

The AEM Screens solution includes the AEM Screens player software that runs on one or multiple screen devices. These devices connect to an AEM Server in order to fetch and play content. The AEM Screens player must be registered with an AEM Author instance through which it receives credentials and then uses basic authentication over HTTPS to periodically check and download content and configuration changes. The player is switched over after registration to an AEM Publish instance that is geographically close to the player.

Playback can be optionally synchronized across multiple screens in one location, such as a video wall. In this case, one device is designated as the 'primary' and sends playback commands to client devices, which then play the content.

.

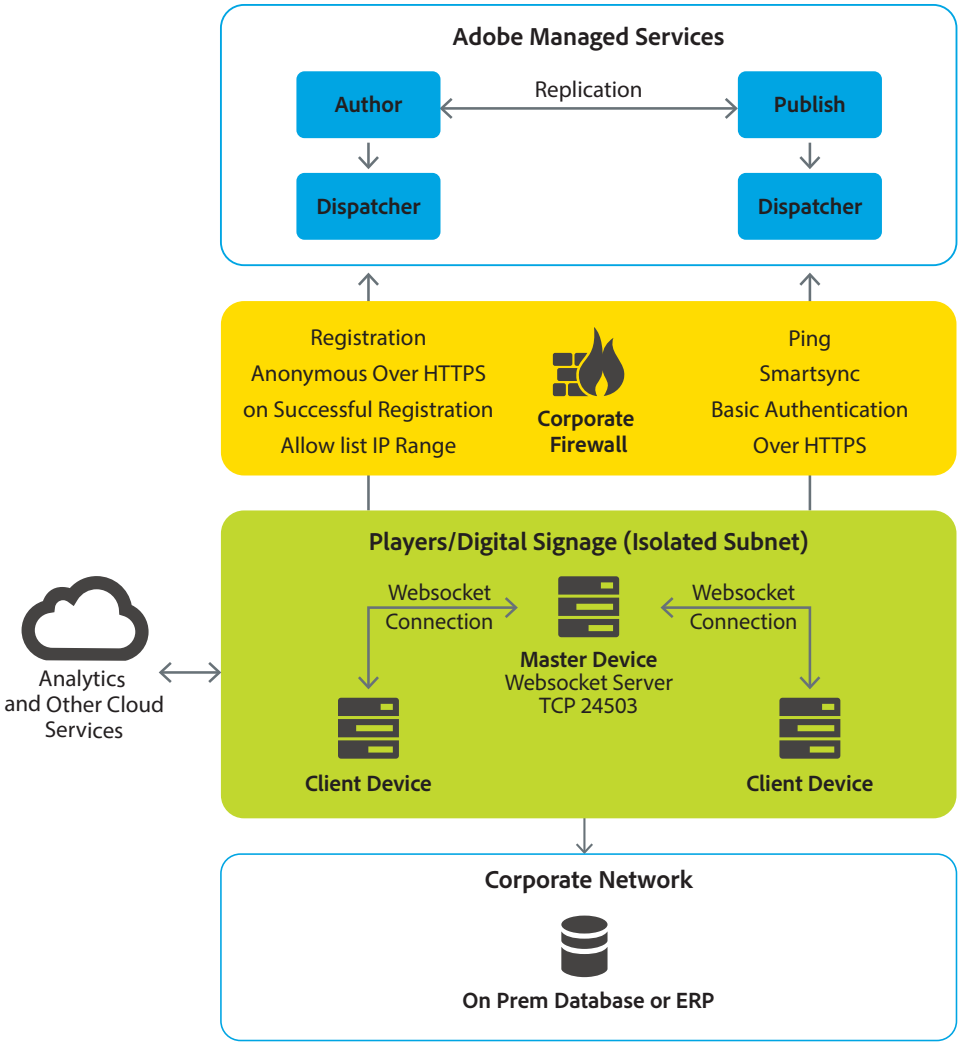

Figure 1: The Adobe Experience Manager Screens solution architecture

NOTE: Websockets are only needed if you are using command sync for synchronized playback. Player connections are outbound only. Players serve local content using a local http server at port 24502. Inbound connection not needed except for debugging.

Adobe Experience Manager Screens Data/Content Flow

The following is how a content author uses AEM Screens to push advertising content to one or more screen devices using AEM Screens:

1. The content author logs into the AEM Author instance and creates an AEM Screens project, including target locations, displays, channels, and schedules. The content author may then include uploaded assets, such as images and videos, to these channels and/or request developers to build SPAs (single page applications), experience fragments, or other dynamic content and include them in the channels.
2. The AEM Screens project—and its associated content—is then published to the AEM Publish instance.
3. An Administrator then configures players (with the AEM Screens player software installed) to point to the AEM Author instance (unauthenticated over https).
4. Then the administrator logs into the AEM Author instance and registers the player that shows up as a pending device. This act of registration creates a username and password for the player. This

username is stored in the AEM user store and is not a federated ID or LDAP or IMS. The administrator can configure the password complexity rules for the players in using the OSGi console in AEM.

5. The generated username and password is then sent to the player that uses these credentials for basic authentication over https for subsequent communication with AEM.
6. At this point, the player is "activated," which replicates the player to the AEM Publish instance and switches it over to an AEM Publish instance that is in close geographic proximity to the device for all future operations.
7. The player uses a "ping" mechanism, which is a periodic request over https to AEM Publish that informs AEM that the player is alive (i.e., heartbeat check) and in response, AEM can send any commands that the player needs to perform, such as taking a screenshot, sending logs, or downloading updated content. This is entirely a pull mechanism using only outbound connections from the player to AEM.
8. In the event that the experience requires synchronized playback on more than one screen, the primary player conducts a "command sync" with the target secondary players through WebSocket connections.

Adobe Experience Manager Screens Player/Device Security

In addition to securing the AEM solution software and AEM Screens player software, the physical, network, and operating system security of the screen devices is important as well. Without taking these into account, a malicious actor could swap out the device playing your content with a different device, which could either connect to your network through physical outlets and/or display malicious content.

For a complete checklist that summarizes the below in actionable steps, please see the AEM Screens Security Checklist.

Physical Security of Screen Devices

- Keep signage devices out of easy reach
- Secure any movable computing unit in a container, if possible. Also secure the cables connecting the device to the internet.
- Seal tablet devices in containers and padlock or otherwise secure the containers to the desk or table on which they reside.
- Consider adding CCTV cameras and/or tamper-proof sensors, based on threat assessment.
- Disable any remote IR ports and other unused USB or serial ports on the computing device.

Network Security for Screen Devices

- **Isolate the subnet on which the signage players reside** — Isolating the devices in a subnet configured to only allow access to network resources that are absolutely necessary for the display of content protects your corporate network from compromise, even if the device and subnet are compromised.
- **Follow best practices for WiFi security (if using)** — While out of scope of this paper, best practice is to configure a separate WiFi network for the signage devices, configured for limited acesss to resources, rather than the corporate WiFi network.
- **Configure the device firewall to only allow outbound connections** — If your device OS includes a firewall, you should configure it to only allow OUTBOUND connections to AEM on the ports configured. No inbound connections should be allowed.[1] Ask your device provider if any additional configurations are required for its firewall software.
- **Use IP allow lists** — Implementing IP allow lists when using AEM Screens helps ensure that only users from a valid IP range can access the AEM server software. Adobe also recommends restricting

[1] If you are using synchronized playback across devices, the device firewalls should be configured to allow the standard WebSocket protocol at TCP port 24503 for the designated primary device, which may also need a static IP (if configured using IP address instead of hostname). In synchronized playback, the primary device sends playback commands to client devices, which then play content. Using an isolated subnet for synchronized playback devices, such as video walls, is also recommended.

access to the AEM Author instance that handles player registration to only allow players from the allowed IP range.

Operating System Security for Screen Devices

Because digital signage players are single-purpose devices, the devices' operating systems must be locked down to only allow the AEM Screens player application to run and do so in kiosk mode. Other overall recommendations include uninstalling all unnecessary applications and disabling unnecessary services and ports. Adobe highly recommends using a central management or device management solution to achieve a full kiosk lockdown of the player OS and device.

OS-specific security instructions follow:

- **For Chrome OS Devices** — Please go to the AEM Screens HelpX on Chrome Management Console.
- **For Windows 10 Devices** — Please go to the AEM Screens HelpX on Implementing Windows 10 Player.
- **For iOS Devices** — Guided access restricts iPads to a single application. After ensuring that the target device is running the latest version of iOS, go to the guided access page to lock the device to the AEM Screens player.
- **For Android Devices** — Please go to the AEM Screens HelpX on Implementing Android Player.

Application Security for Screen Devices

The Adobe Screens player application has an Admin UI for modifying configurations, including the server URL. Ideally, all configurations should be provisioned using a device manager and, after registration, be managed with AEM. This requires users to disable the Admin UI, channel switcher, and activity UI in the player configuration when deploying in production. If the player configurations are managed by a device manager, they are enforced by policy and cannot be overridden at the local level.

If the player configurations are not managed by a device manager, security of the devices relies on the physical and OS security, as described above.

Content Integrity — The AEM Screens player conducts delta downloads of content changes for offline playback, using hashes to check the integrity of downloaded files.

Player Registration — When pointed to an AEM Author instance, the AEM Screens player enters the unregistered state and displays a code, using an unauthenticated registration service on the AEM Author instance. To ensure against malicious actors pointing rogue devices to your AEM Author instance, you should consider having the instance inside your firewall for on-premise instances and for AMS use allow lists so only listed IPs can access the AEM Author instance.

When registering, verify the code on the device matches the one on the server. Alternatively, you can have the devices pre-registered by an audio/video integrator.

Monitoring — AEM Screens provides a monitoring email that can be configured to notify you if any device/s have not checked in with the AEM Server for a configurable period of time. If you feel any registered player is lost, stolen, or otherwise compromised, simply select that player and delete it in the device dashboard; the user associated with the player will be deleted. After this, the device will no longer be able to authenticate using AEM. You can also deregister the device in the MDM so it can no longer access the network.

Data Security for Screen Devices

Data in transit between AEM Sites instances and AEM Screens players are conducted over secure, encrypted connections using TLS. Data at-rest is encrypted by the cloud service provider.

Securing data in motion — You must use HTTPS and use a valid certificate signed by a known certifying authority to ensure the security of communication between the player and AEM. Please use TLS and not SSL v3 that has been compromised.

Securing data at rest — The player uses different storage mechanisms for player configuration including credentials based on the type of player and operating system. Please see the table below. This provides sufficient security when the device is managed and configured in Kiosk mode. However, we do not recommend storing any sensitive information including personally identifiable information (PII) or personal health information (PHI) on these devices.

	Preferences	Content
Chrome OS	Chrome.storage.local	HTML5 File system
Windows	%appdata%	%appdata%
iOS	NSUserDefaults	Cordova.file.datadirectory
Android	SharedPreferences	Cordova.file.datadirectory

Adobe Experience Manager Screens Authentication

Access to AEM Screens requires authentication with a username and password. We continually work with our development teams to implement new protections based on evolving authentication standards.

The IDs below are only applicable to human users. The player's user credentials are in the standard AEM user store. Users can access AEM Screens in one of two different types of user-named licensing:

Enterprise ID is an Adobe-hosted, enterprise-managed option for accounts that are created and controlled by IT administrators from the customer enterprise organization. While the customer organization owns and manages the user accounts and all associated assets, Adobe hosts the Enterprise ID and performs authentication. Admins can revoke access to Adobe Experience Manager Screens by taking over the account or by deleting the Enterprise ID to permanently block access to associated data.

Federated ID is an enterprise-managed account where all identity profiles—as well as all associated assets — are provided by the customer's Single Sign-On (SSO) identity management system and are created, owned, controlled by customers' IT infrastructure. Adobe integrates with most any SAML 2.0-compliant identity provider.

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

Adobe Experience Manager Screens Roles and Permissions

Please follow the detailed guide on managing role-based access control (RBAC) for player devices, experience authors and screens administrators.

Whenever a player is registered against an AEM instance, a user is created for that player device and the credentials are sent to the player. This username can be used to uniquely identify a player device after registration.

Players that are registered against a particular project are stored in a group called screens-<project>-devices where project is the name of the screens project. All these project groups are under the screens-devices-master group. The ACL of these project devices groups can be adjusted to access the content you need.

You may want a content author to only see and edit the content for which they are responsible. The best practice is to follow the standards of minimal access required to perform the task on hand.

Adobe Experience Manager Screens Hosting and Security

The Adobe Experience Manager solution is hosted on Adobe-leased data centers in the U.S, (Virginia) and in Amsterdam, The Netherlands and Sydney, Australia.

Figure 2 — Adobe AEM Screens hosting locations

Adobe Experience Manager Screens Network Management

Adobe understands the importance of securing the data collection, data content serving and reporting activities over the AEM Screens network. To this end, the network architecture is designed with security as a top priority, including segmentation of development and production environments and authenticated RBAC.

Segregating Client Data

Content is placed into separate databases. In some cases, more than one client may share a cloud cluster, but the content is segmented into separate databases. The only access to these servers and databases is via secure access by the AEM Screens application. All other access to the application and content servers is made only by authorized Adobe personnel and is conducted via encrypted channels over secure management connections.

Secure Management

Adobe deploys dedicated network connections from its corporate offices to its data center facilities in order to enable secure management of AEM Screens. All management connections to the servers occur over encrypted TLS channels only accessible from the Adobe corporate network. All access requires two-factor authentication.

Firewalls (Secure Network Routing) and Load Balancers

Secure network routing is implemented to only allow connections to allowed ports, i.e., Port 443 for HTTPS. Outbound traffic is only allowed on HTTPS and NAT masks the true IP address of a server from the client connecting to it. The load balancers proxy incoming 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 NAT and internal network policies, prevent an individual server on the network from being directly addressed from the Internet, greatly reducing the potential vectors of attack.

Intrusion Detection

Adobe deploys Intrusion Detection System (IDS) sensors at critical points in the AEM Screens network to detect and alert our security team to unauthorized attempts to access the network. The security team follows up on intrusion notifications by validating the alert and inspecting the Adobe Experience Manager Screens platform for any sign of compromise. Adobe regularly updates all sensors and monitors them for proper operation.

Service Monitoring

Adobe monitors all our servers, routers, switches, load balancers, and other critical network equipment on the Adobe Experience Manager 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 promptly 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.

Further, Adobe Experience Manager Screens uses state of the art technologies and industry-leading providers for application specific monitoring and alerting. SLIs and SLOs are constantly tracked and violations result in alerts with the right severity.

Data Backups

Adobe backs up customer data for AEM Screens daily using snapshots. Each snapshot is stored up to seven (7) days. The combination of backup procedures provides quick recovery from short-term backup as well as off-site protection of data.

Change Management

Adobe uses a change management tool to schedule modifications, helping increase communication between teams that share resource dependencies and inform relevant parties of pending changes. In addition, Adobe uses the change management tool to schedule maintenance blackouts away from periods of high network traffic.

Patch Management

In order to automate patch distribution to host computers within the AEM 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.

For AEM Screens instances, product updates, including security updates, are applied through the deployment pipeline (see above section on the deployment model for more details).

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 Adobe Experience Manager production server connections for auditing. ForAEM Screens users, Adobe makes built-in security features available to implement permissions and access control using groups and privileges.

Logging

In order to help protect against unauthorized access and modification, Adobe captures and manages network logs, OS-related logs, and intrusion detections using industry-standard tools. Adobe periodically reviews log storage capacity and expands storage capacity if, and when, required. Adobe hardens all systems that generate logs and restricts access to logs and logging software to authorized Adobe personnel. Adobe retains raw logs for one year and all logs are managed and accessed only by Adobe personnel. Customers can also retrieve AEM Screens logs (e.g. access log, debug log) from Cloud Manager.

Additionally, customers can retrieve the player device logs from AEM as well as configure the log level per device, which is set to "warning" by default. If Adobe customer support is required in order to troubleshoot an individual device, the support engineer will set that device's log level to debug, reproduce the issue, and collect the logs directly from AEM. The customer can define how many logs are retained; The default is 10 files of 1MB each. After 1MB, a new log file is created, and when 10 files are reached, the entire log is overwritten.

Data Center 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 Experience Manager Screens 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 promptly handle environmental issues 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 Experience Manager Screens 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 one of Adobe's data collection environments is unavailable due to 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 provide an effective and accurate recovery.

Failover Process

When an event is determined to result in long-term data collection disruption, Adobe will reconfigure DNS to send data collection requests to a secondary location not affected by the disaster. Adobe will also manually place a hold on data processing in the primary environment

to preserve the chronological order of page views, which is necessary for the recovery process

to work successfully.

DNS record TTL (time to live) is set to allow this switch to the secondary location to happen quickly. For customers using Regional Data Collection ("RDC"), data collection will continue to queue data without intervention should the Data Processing Center be temporarily unavailable. If an RDC site should fail, data collection will continue to the other RDC sites. While data collection is in a failover mode, customers are notified of the ongoing situation with regular status updates. If it is expected that the primary data collection location will be back online within five business days, no historical data will be transferred to, or data collection processed at, the secondary location. If the disaster at the primary data collection location is serious enough to have destroyed or make 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 page views will be processed sequentially in time order. During page view processing, the application will be available but reports will not be available in real time until page view processing is complete. Page view processing will take approximately one day for every four hours the failover process was active. Time required to recover historical data from off-site may take up to an additional ten (10) days.

The Adobe Security Organization

As part of Adobe's commitment to the security of its 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 Experience Manager 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.

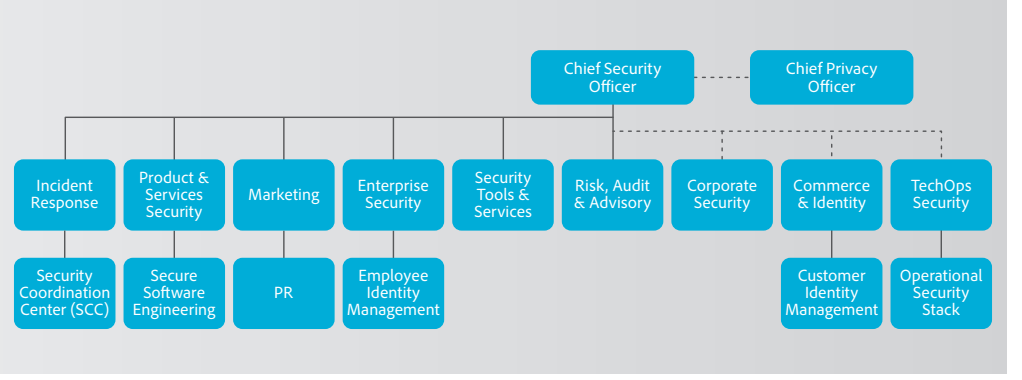

Figure 3: The Adobe Security Organization

Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe Experience Manager 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 Adobe Experience Manager 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 Experience Manager 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

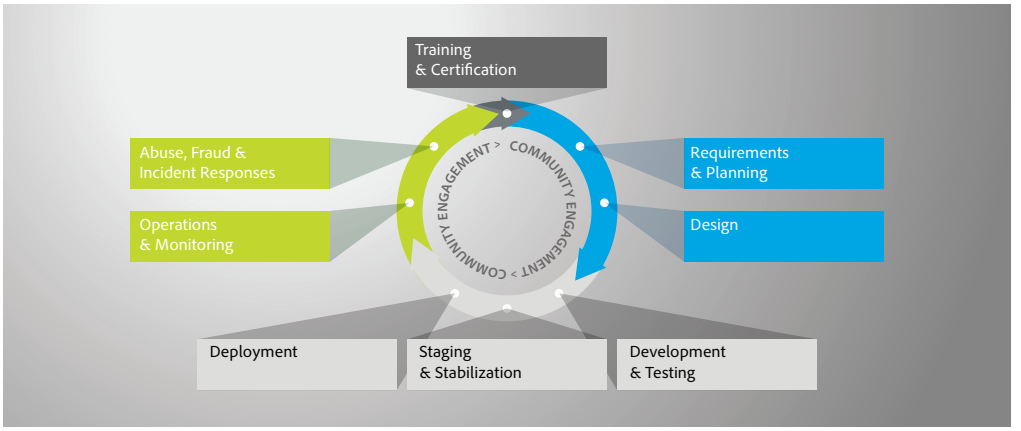

Figure 4: The Adobe Software Product Lifecycle (SPLC)

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 three levels, each designated by a colored 'belt': white, brown, and black.

The white level is 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 Adobe Experience Manager 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 Experience Manager Screens 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.

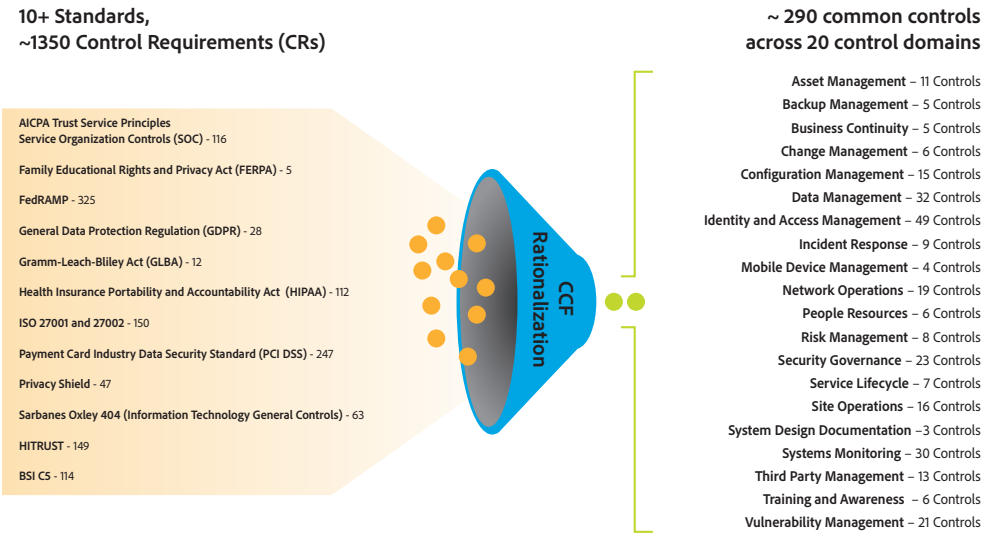

Figure 5: The Adobe Common Controls Framework (CCF)

Current Regulations and Compliance for Adobe Experience Manager Screens

For the most up-to-date information about Adobe Experience Manager Screens compliance, please see the Adobe Compliance List.

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.

Adobe Risk & Vulnerability Management

Adobe strives to ensure that its risk and vulnerability management, incident response, mitigation, and resolution process is nimble and accurate. Adobe continuously monitors the threat landscape, shares knowledge with security experts around the world, swiftly resolves incidents when they occur, and feeds this information back to its 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. Adobe conducts a full penetration test annually.

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.

Internally, the Adobe Experience Manager security team performs a risk assessment of all Adobe Experience Manager components quarterly and prior to every release. The Adobe Experience Manager security team partners with technical operations and development leads to help ensure all high-risk

vulnerabilities are mitigated prior to each release. For more information on Adobe penetration testing procedures, see the Adobe Secure Engineering Overview white paper.

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 see the Adobe Incident Response Overview.

Forensic Analysis

For incident investigations, the Adobe Experience Manager team adheres to the Adobe forensic analysis process that includes, as appropriate, complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody record.

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.

Virus Protection

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

Adobe Employees

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

Employee Access to Customer Data

Adobe maintains segmented development and production environments for Adobe Experience Manager, 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 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 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.

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 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 Adobe Experience Manager Screens 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 security our customers' data.

For more information, please visit the Adobe Trust Center.

Adobe

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