WHITE PAPER

Adobe Identity Management Services Security Overview

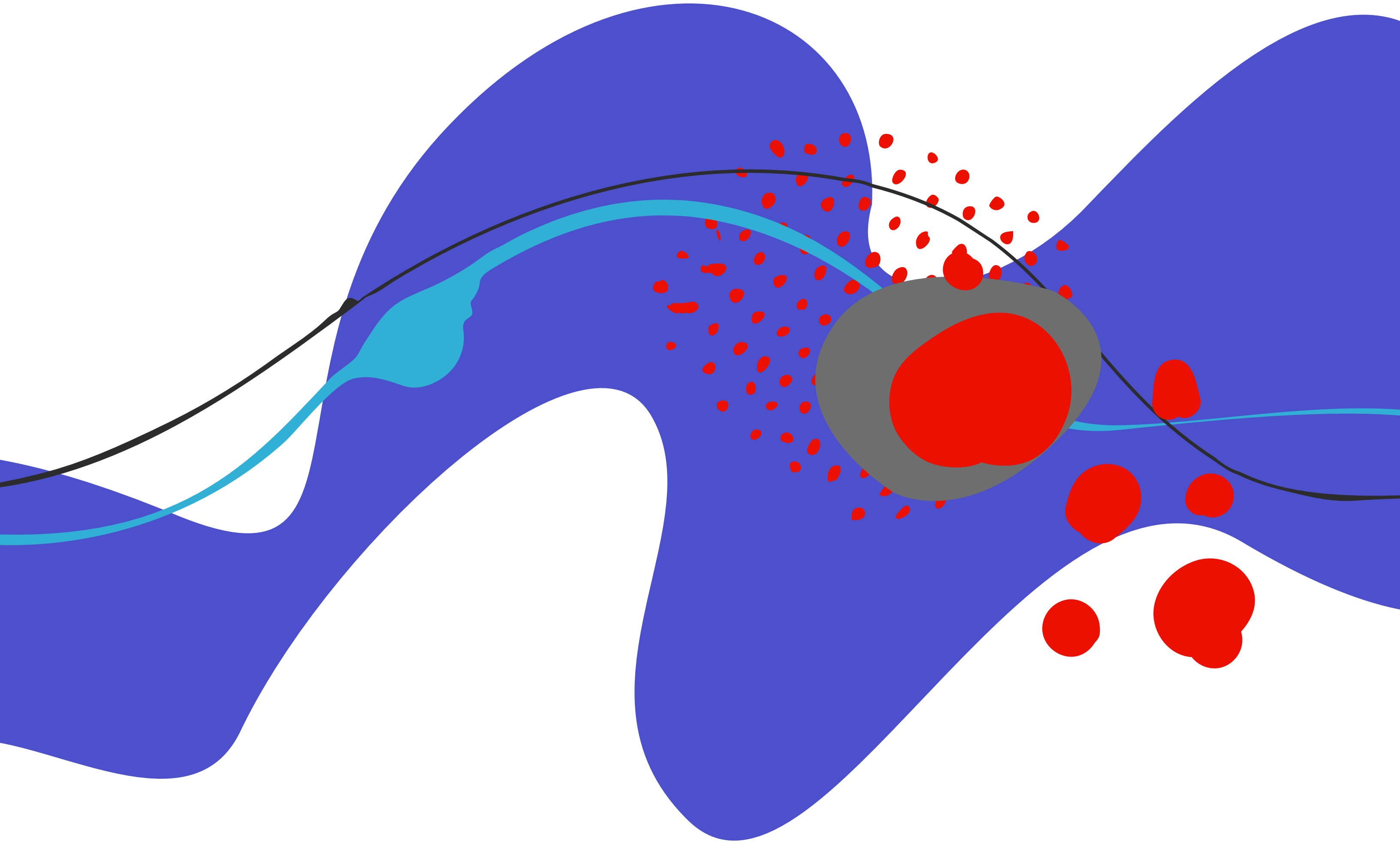
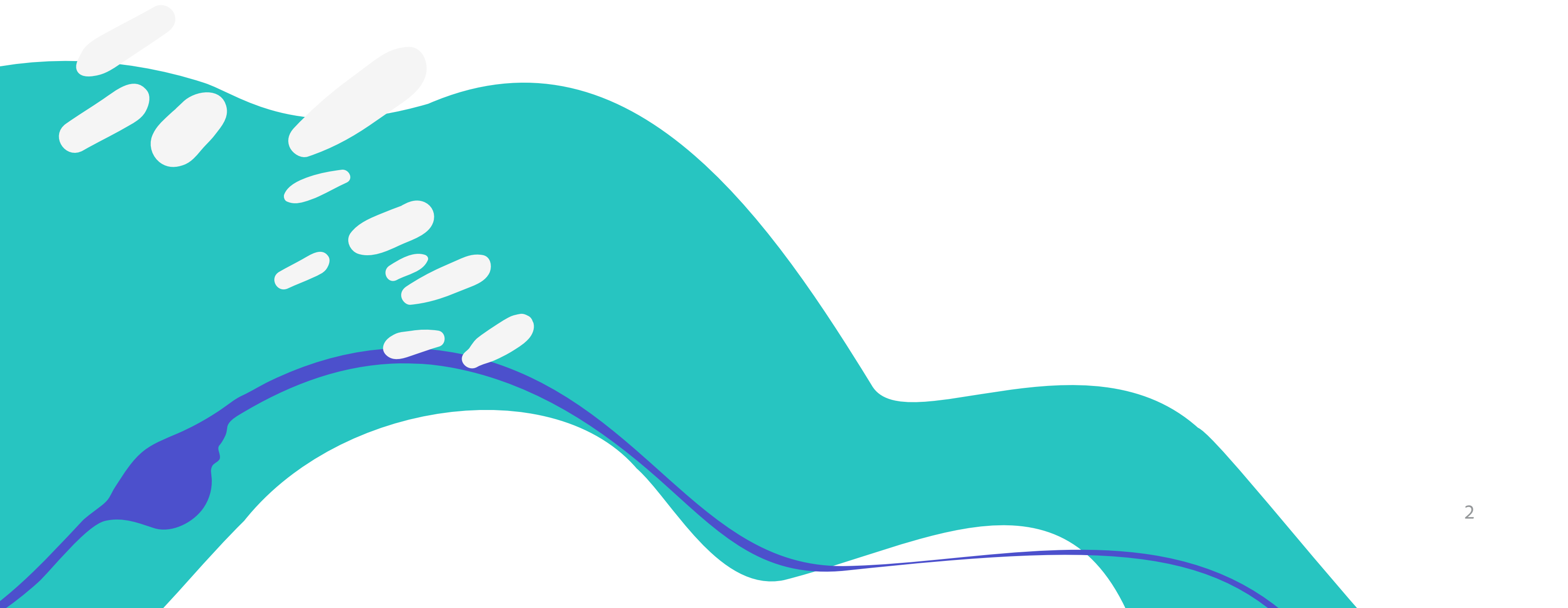


Table of Contents



Adobe Security

At Adobe®, we take the security of your digital experiences seriously. Security practices are ingrained into our internal software development and operations processes and tools, and the Adobe Secure Product Lifecyle (SPLC) controls are implemented by our cross-functional teams to help 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 continually work to incorporate advanced security technologies and practices into the products and services we offer.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to help bolster the security of your Adobe Identity Management Services experience and your data.

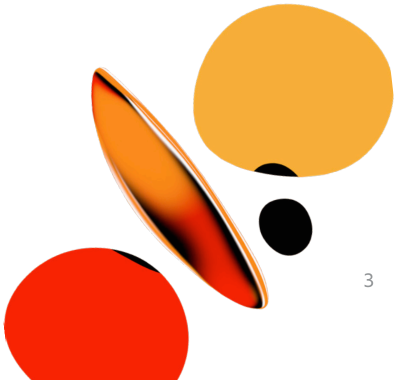
About Adobe Identity Management Services

Adobe Identity Management Services (IMS) handles end-user authentication for every Adobe solution and consists of three (3) components:

- **Adobe Identity Service** — Handles authentication and validation of end-users, including federation and runtime Single Sign-On (SSO);
- **Adobe Admin Console** — Provides a central location for managing Adobe entitlements across the entire organization. The Adobe Admin Console handles user management, cloud service and desktop license entitlement, federation configuration, and data loss prevention security; and
- **Adobe User Management API (UMAPI)** — Allows organizations to manage enterprise users and entitlements in the Adobe Admin Console at the API level.

Named User Licensing

The Adobe IMS platform manages entitlements and unique identifiers, also called "named user licensing," allowing end-users to authenticate themselves to their deployed Adobe desktop applications and cloud services.



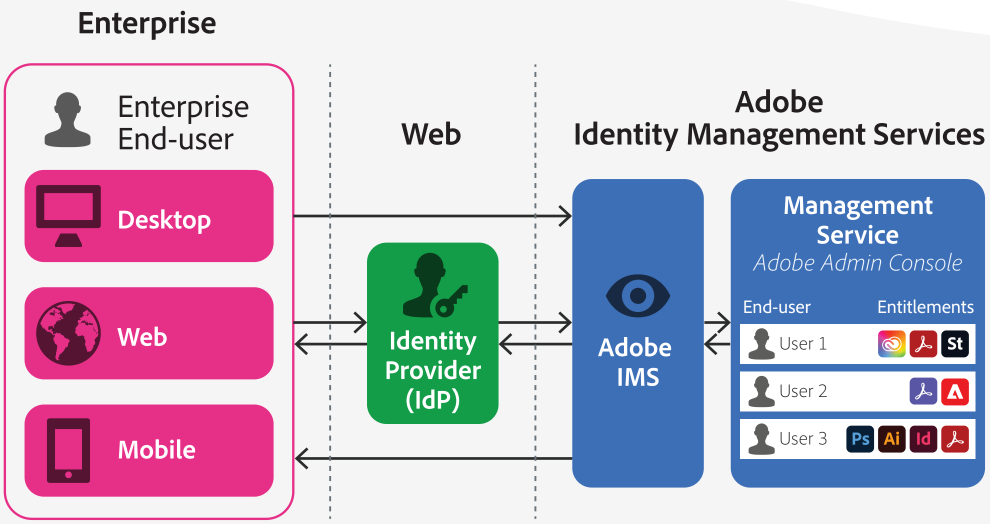


Figure 1: Adobe Identity Management Services Architecture

Figure 1 (above) depicts the interaction of an end-user with the Adobe IMS using named user licensing. In the example, the end-user has installed Adobe applications on their desktop or mobile device/s. When an end-user attempts to activate or launch an Adobe desktop or mobile application or access an Adobe cloud service, that endpoint communicates with the Adobe IMS.

Based on the named user identity type (see next section), Adobe IMS either allows the end-user to log in directly or passes control to the customer's identity provider (IdP), which performs a federated SSO authentication. On successful authentication, Adobe IMS verifies the end-user's entitlements and completes their requested action. The named end-user can now use the software or services to which they are entitled.

User Identity Types

For enterprise deployments, Adobe supports three (3) named user identity types:

Business ID is an Adobe-hosted, enterprise-managed option for organizations that either use email addresses outside of their own claimed domain as the user's ID or for customers that have not claimed a domain for identity purposes. Adobe Business ID is the preferred option for organizations that work with outside contractors or freelancers who do not have an organizational ID or email.

Enterprise ID is an Adobe-hosted, enterprise-managed option for accounts that are created by IT administrators from the enterprise organization. The organization owns and manages the user accounts and all associated assets. User accounts are managed through the Adobe Admin Console and/or the UMAPI. Administrators can set authentication policies for these users, but Adobe fully manages the user's authentication and credentials.

Federated ID is an enterprise-managed account in which all identity profiles are provided by a Single Sign-On identity management system and are created, owned, and controlled by the enterprise IT organization. Adobe integrates with any SAML 2.0-compliant identity provider. User accounts are authenticated through the identity provider and authorized via the Adobe Admin Console. The organization's identity provider completely controls setting and enforcing authentication policies. Adobe also supports connection to and synchronization with Microsoft Azure Active Directory and Google Workspace Directory services via OpenID Connect for federated identity services.

Most enterprise organizations use Enterprise or Federated IDs for their employees, contractors, and freelancers, provided their email is within the companies' claimed domains. Adobe recommends the use of Business IDs if the end-user email is not within a company domain. For more detail, please see the Identity Types page on Adobe HelpX.

Better suited for individual or personal use, Adobe does not recommend the use of the Adobe ID identity type for enterprise deployments.

User Identity Management

Enterprise customers can manage user identities either manually or automatically.

Manual Identity Management

Administrators can manually manage users either individually by adding, deleting, or changing users one at a time within the Adobe Admin Console or in bulk by uploading a CSV spreadsheet of users into the Adobe Admin Console.

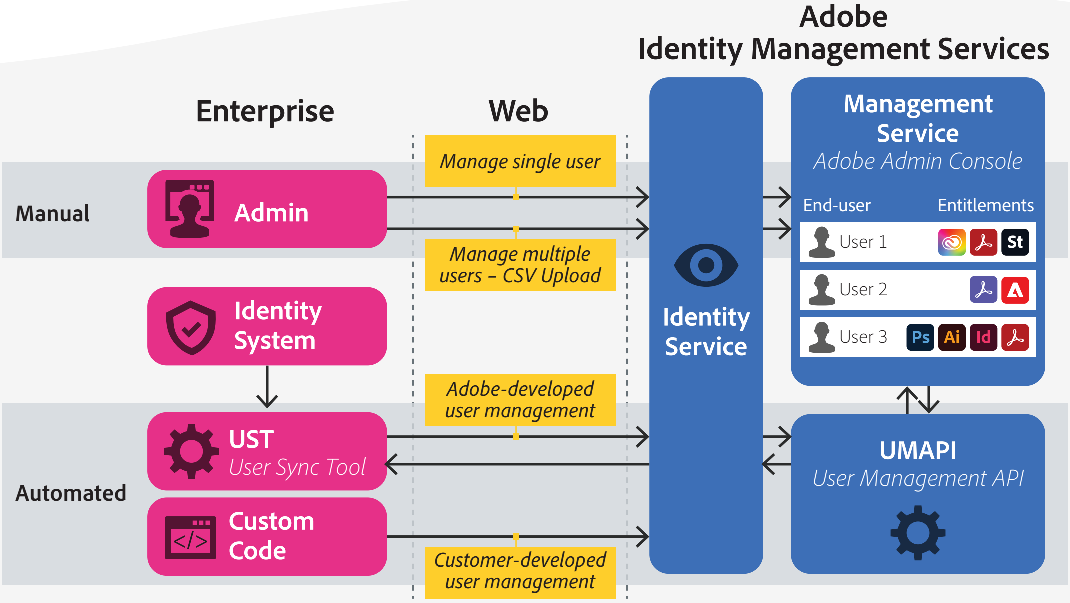


Figure 2: User Identity Management Options

Automated Identity Management

If an administrator wishes to automatically manage users, they can do so in one of three (3) ways:

- Programmatically add, update, or remove users via custom-developed code using **UMAPI**.
- Synchronize all users with Microsoft Azure Active Directory and Google Workspace Directory services using the **SCIM (System for Cross-domain Identity Management)** open standard for cloud-based synchronization.
- Synchronize specific users from the enterprise directory and then add users to or remove users from appropriate license pools in the Adobe Admin Console using the **Adobe User Sync Tool (UST)**, a set of Python scripts developed and maintained by Adobe.

User Sync Tool

The UST reads identity data from all Lightweight Directory Access Protocol (LDAP) groups in the enterprise's directory service, such as Microsoft Active Directory and other directories supported by OpenID Connect, and makes secure REST calls to UMAPI to create, update, or delete users on Adobe's servers.

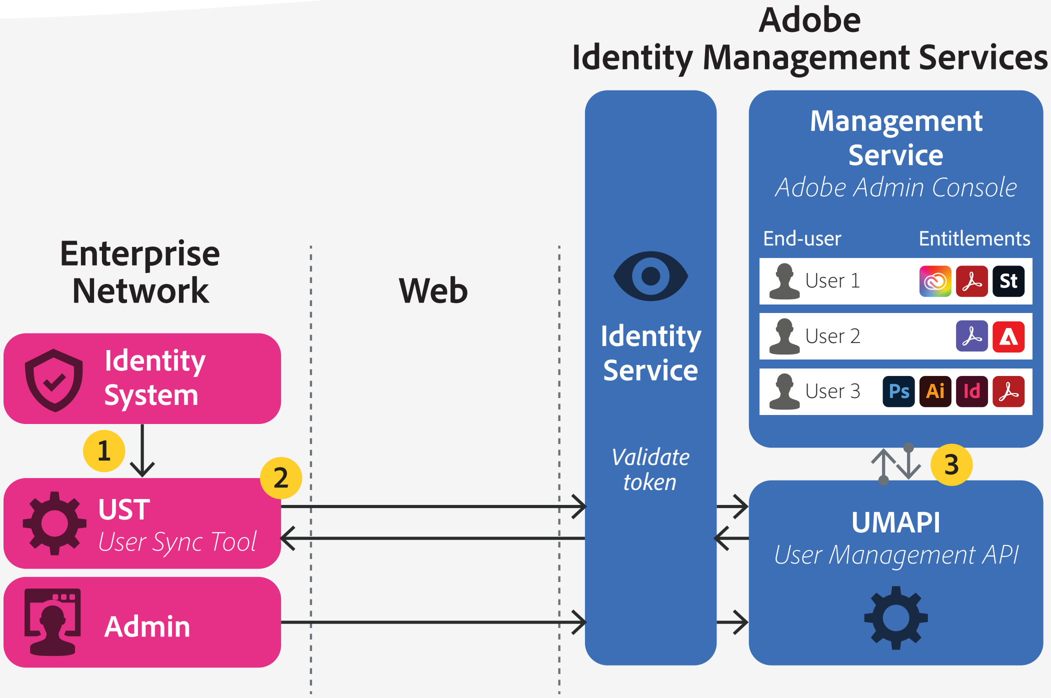


Figure 3: The User Sync Tool (UST)

Each time the UST runs, it:

1. Requests employee records from groups within the enterprise's directory. The groups and LDAP query can be customized to fit the enterprise's specific environment;
2. Requests current users and associated product configurations from the Adobe Admin Console. The UST connects to the UMAPI via REST calls over HTTPS utilizing a verified, time-boxed access token, which is generated from a signed, encoded JWT (JSON Web Token);
3. Determines which users need to be created, deleted, or updated based on rules defined in the configuration files; and
4. Makes the required changes to the Adobe Admin Console through the UMAPI, entitling users to the appropriate software and services.

The UST can automatically keep enterprise users' Adobe entitlements in sync with their groupings in the directory service. For example, if a user is added to the LDAP directory, the next time the UST runs, the UMAPI pulls the user's information from the directory and adds it to the appropriate group within the Adobe Admin Console. If a user is changed or removed from the LDAP directory, the UST will call the UMAPI and perform the appropriate action in Adobe Admin Console.

More detailed instructions about how to install, register, and run the UST can be found on the Set up the User Sync Tool page on Adobe HelpX.

More detail about managing users is available on the Adobe Admin Console users page on Adobe HelpX.

User Authentication and Authorization Data Flow

Adobe enables user authentication and authorization in two (2) ways:

Interactive authentication and authorization occurs when a user explicitly signs into an Adobe desktop application or cloud service and enters their information into a dialog box in the user interface. In this case, authorization occurs seamlessly and, to the end-user, appears to be part of the authentication process.

Adobe also supports multi-factor authentication (MFA), which provides an extra layer of security by requiring end-users to enter additional pieces of knowledge specific to them after the end-user has been authenticated using the initial two-step verification in the UI. Adobe offers policies to enforce MFA for Adobe ID and Business ID users. Even when MFA is deployed, authorization occurs seamlessly and, to the end-user, appears to be part of the authentication process.

Automated authentication and authorization occurs after an end-user has been initially authenticated using interactive authentication. Automated authentication utilizes a unique identification token so that the end-user does not have to log in again through the duration of the session, and authorization occurs seamlessly as well. Any time an end-user interacts with an application or service and is not required to explicitly log in, that end-user is taking advantage of automated authentication. When a user logs out of a session, authorizations are re-checked on their next login to verify access rights.

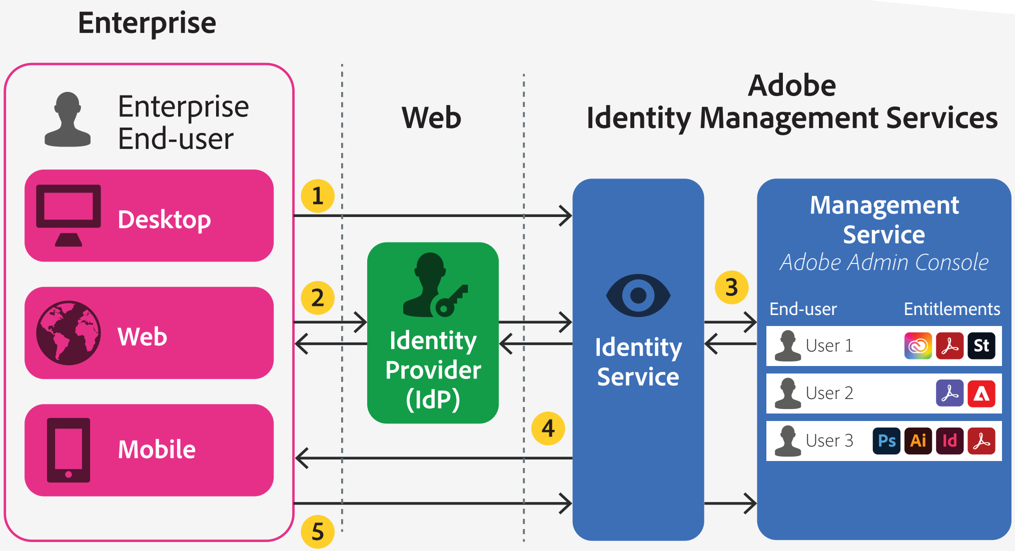


Figure 4: Adobe User Authentication Data Flow

While the user authentication data flow depends on the specific user identity type, the authentication process typically includes the following steps, which map to the numbers in the diagram above:

1. The end-user launches a desktop application or requests access to an Adobe cloud service for the first time. If they are using a Business ID or Enterprise ID, they log in using Adobe IMS.
2. If the organization uses Federated ID, when the end-user enters their email address or just the domain (e.g., @companydomain) in the username field, Adobe IMS initiates a SAML request, which redirects the end-user to their identity provider to log in using their corporate credentials.
3. Once the user is properly authenticated, Adobe IMS then conducts the required entitlement and policy enforcement checks and redirects the user to the appropriate Adobe cloud service or enables appropriate desktop application licensing.
4. Adobe IMS stores a device token on the end-user's computer and uses it to generate an access token (similar to an application session token). Together, these two tokens are used to generate a signed license for the application, which is encrypted and stored with the device token in the end-user's settings. Because the token is operating system-independent, if the user reboots their system, they do not need to re-authenticate themselves to the Adobe desktop application or cloud service.

5. At this point, the end-user can concurrently use any Adobe desktop application or cloud service without manually re-authenticating themselves into each separate application (i.e., automated authentication). When the user launches a new desktop application in the same session, it contacts Adobe IMS and exchanges the device ID and device token for an access token. Policy checks and entitlement confirmations occur during this process. If, for any reason, a user's access rights or entitlements are changed or revoked, access tokens and device tokens become invalid.

Adobe offers optional administrative policies that further limit the lifespan of access tokens by requiring more frequent authentication, which can be useful for certain Adobe Experience Cloud applications. However, Adobe does not recommend using these policies unless an enterprise has specific security requirements.

Identity Data

What data do we collect and why?

Adobe collects identity data ensuring each end-user has a unique ID to verify them for license entitlement purposes and allow password protection of those entitlements as well as the content generated and stored by the user. For identity data, Adobe collects:

- **Username and domain** — An identifier for the user, typically a valid, primary email address in user@domain format. For Business ID and Enterprise ID types, the full username is required to log into Adobe applications and cloud services. Some enterprises employ usernames that don't match their email addresses (e.g., firstnamelastname vs. user@domain), however, this is controlled by the enterprise. For Federated ID identity types, either the full email or just the @domain portion is required to pass control to the proper identity provider.

- **UID (Federated IDs only)** — A unique identifier associated with the user (usually the email address); Adobe uses the UID as a key from the identity provider to look up the end-user in Adobe IMS.

- **Password (Business ID and Enterprise ID only)** — Passwords are hashed according to industry best practices before storage. Adobe never retains a copy of a user's password in a format that could be decrypted into a user's plaintext password.

- **Date of Birth (Adobe ID only)** — Required for Children's Online Privacy Protection Act (COPPA), General Data Protection Regulation (GDPR), and age verification for website access.

- **Country Code** — The ISO Alpha-2 and ISO Alpha-3 country codes for the user are gathered when the identity profile is created. Adobe generally uses the country code to determine the regional asset storage location for user-generated content. Enterprise ID and Federated ID locations are defined by the organization.

- **First Name and Last Name** — Gathered when the identity profile is created. For Enterprise ID and Federated ID identity types, the UID, Country Code, First Name, and Last Name fields are configurable by the IT administrator when creating the user accounts. Administrators can also determine how much or how little user information is included in those fields.

Where do we store your identity data?

Regardless of the geographic location of the customer, all identity data is stored in multi-region, load-balanced, cloud infrastructure providers with data centers located in North America (Oregon and Virginia), Europe (Ireland), and APAC (Singapore). Identity data is replicated across all data centers for reliability reasons.

How do we secure your identity data?

All identity data is secured at-rest using AES-256-bit encryption in compliance with the Adobe Common Compliance Framework (CCF) and meets our internal policies for encryption and storage of sensitive data.

How long do we store identity data?

Content is replicated to and backed up within each data center, in other data centers within the region, and in cross-region data centers for load balancing and redundancy. Data center backups for identity data occur daily and are stored for seven (7) days. Adobe also complies with applicable laws regarding cross-border data transfers.

Adobe ID accounts are created, owned, and controlled by the individual user. Accordingly, the individual user controls the lifecycle of the account, apart from the retention policy stated in the Consumer Personal Information Retention Standard (CPIR) maintaining that Adobe ID and Business ID identity types exceeding four (4) years of inactivity are not retained and are deleted. Adobe deactivates Adobe ID accounts and deletes the personal information, hashed password, and payment data associated with it upon request by the individual user or after 48 consecutive months of inactivity.

For both Enterprise ID and Federated ID identity types, the account deletion schedule is determined by the enterprise customer and can be controlled within the Adobe Admin Console. When an enterprise no longer wishes to have a specific Enterprise or Federated ID associated with the enterprise's account, an authorized administrator can remove it within the Adobe Admin Console. More details can be found on the Adobe Admin Console users page on Adobe HelpX.

How do we handle logging?

Adobe logs the following user actions:

- When a user activates their Adobe application or service
- When a user signs into an Adobe application or service
- When a user opens an Adobe application on their desktop or mobile device
- When a user uses cloud storage or services

Log data collected may include the user ID, email address, and IP address of the user, as well as event tracking data. Adobe may also log analytics data related to the application and services usage. A user may opt out of analytics collection at any time.

Who can access your identity data?

Only authorized Adobe personnel have access to identity data and only on an as-needed, least- privileged basis, consistent with Adobe's ISO 27001 certification. Data logged by Adobe IMS is considered "most privileged" (per the Adobe Data Classification and Handling Standard) and is only accessible by an even more restricted number of Adobe personnel.

Adobe Security Program Overview

The integrated security program at Adobe is composed of five (5) centers of excellence, each of which constantly iterates and advances the ways we detect and prevent risk by leveraging new and emerging technologies, such as automation, AI, and machine learning.

Application Security
Operational Security
Enterprise Security
Compliance
Incident Response

Figure 5: Five Security Centers of Excellence

The centers of excellence in the Adobe security program include:

- **Application Security** — Focuses on the security of our product code, conducts threat research, and implements bug bounty.
- **Operational Security** — Helps monitor and secure our systems, networks, and production cloud systems.
- **Enterprise Security** — Concentrates on secure access to and authentication for the Adobe corporate environment.
- **Compliance** — Oversees our security governance model, audit and compliance programs, and risk analysis; and
- **Incident Response** — Includes our 24x7 security operations center and threat responders.

Illustrative of our commitment to the security of our products and services, the centers of excellence report to the office of the Chief Security Officer (CSO), who coordinates all current security efforts and develops the vision for the future evolution of security at Adobe.

The Adobe Security Organization

Based on a platform of transparent, accountable, and informed decision-making, the Adobe security organization brings together the full range of security services under a single governance model. At a senior level, the CSO closely collaborates with the Chief Information Officer (CIO) and Chief Privacy Officer (CPO) to help ensure alignment on security strategy and operations.

In addition to the centers of excellence described above, Adobe embeds team members from legal, privacy, marketing, and PR in the security organization to help drive transparency and accountability in all security-related decisions.

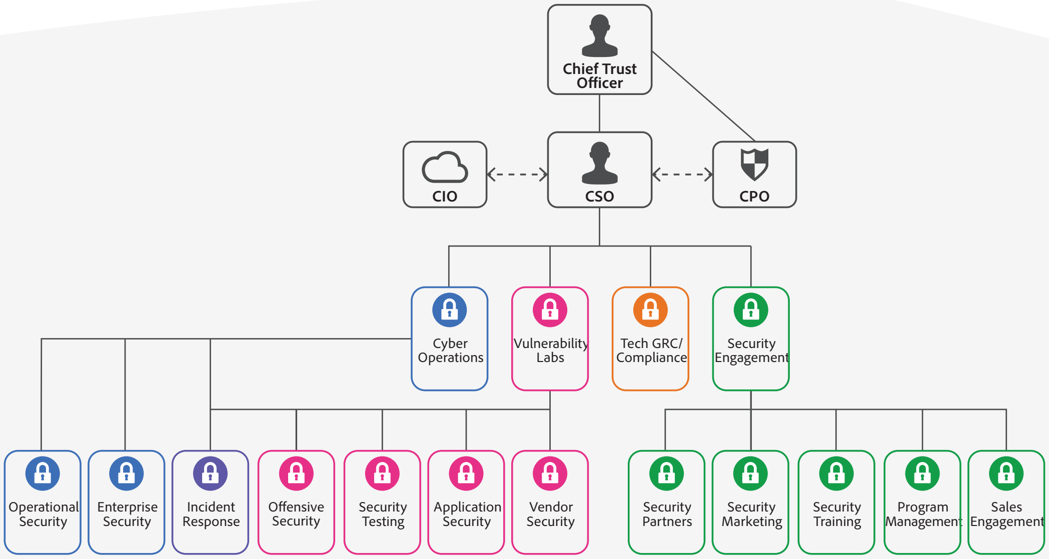


Figure 6: The Adobe Security Organization

As part of our company-wide culture of security, Adobe requires that every employee completes our security awareness and education training, which requires completion and re-certification on an annual basis, helping ensure that every employee contributes to protecting Adobe corporate assets as well as customer and employee data. On hire, our technical employees, including engineering and technical operations teams, are auto-enrolled in an in-depth 'martial arts'-styled training program, which is tailored to their specific roles.

Adobe's culture of security and training programs are outlined in more detail in the Adobe Security Culture white paper.

The Adobe Secure Product Lifecycle

Integrated into several stages of the product lifecycle—from design and development to quality assurance, testing, and deployment— the Adobe Secure Product Lifecycle (SPLC) is the foundation of all security at Adobe. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC defines clear, repeatable processes to help our development teams build security into our products and services and continuously evolves to incorporate the latest industry best practices.

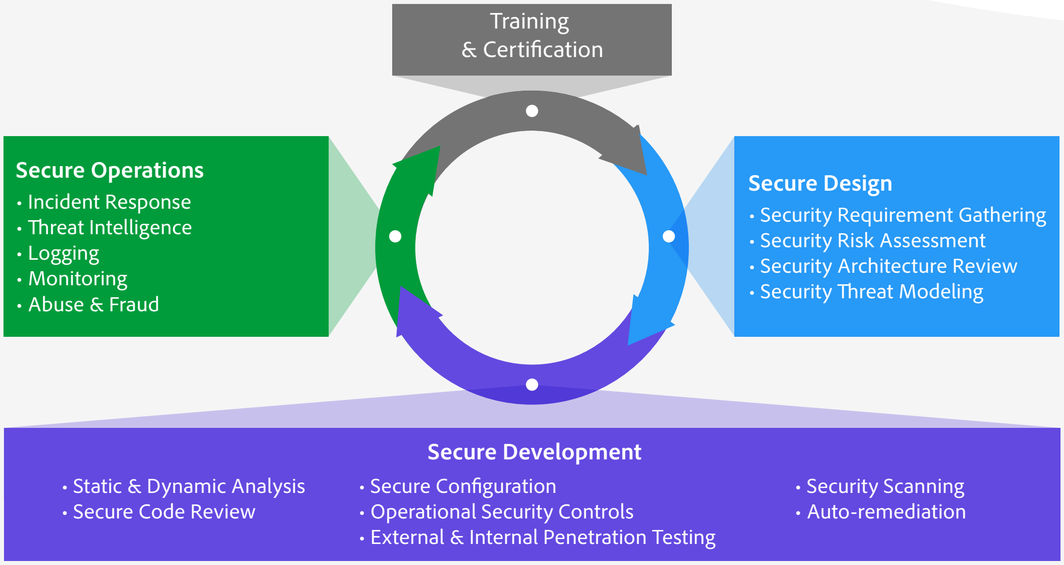


Figure 7: The Adobe Secure Product Lifecycle

Adobe maintains a published Secure Product Lifecycle standard that is available for review upon request. More information about the components of the Adobe SPLC can be found in the Adobe Application Security Overview.

Adobe Application Security

At Adobe, building applications in a "secure by default" manner begins with the Adobe Application Security Stack. Combining clear, repeatable processes based on established research and experience with automation that helps ensure consistent application of security controls, the Adobe Application Security Stack helps improve developer efficiency and minimize the risk of security mistakes. Using tested and pre-approved secure coding blocks that eliminate the need to code commonly used patterns and blocks from scratch, developers can focus on their area of expertise while knowing their code is secure. Together with testing, specialized tooling, and monitoring, the Adobe Application Security Stack helps software developers to create secure code by default.

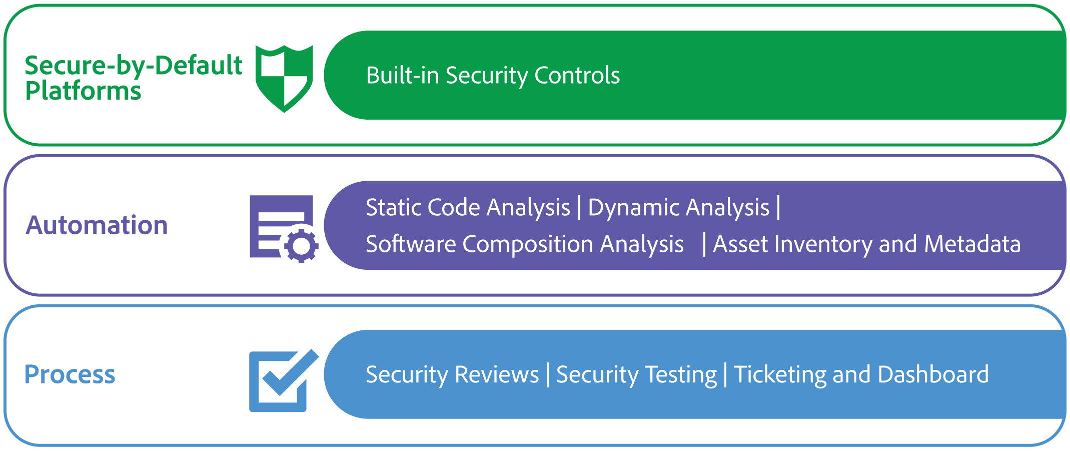

Secure-by-Default Platforms
Built-in Security Controls
Automation
Static Code Analysis | Dynamic Analysis |
Software Composition Analysis | Asset Inventory and Metadata
Process
Security Reviews | Security Testing | Ticketing and Dashboard

Figure 8: The Adobe Application Security Stack

Adobe also maintains several published standards covering application security, including those for work specific to our use of Amazon Web Services (AWS) and Microsoft Azure public cloud infrastructure. These standards are available for view upon request. The Adobe Application Security Overview contains more detailed information about Adobe's application security practices and processes.

Adobe Operational Security

To help ensure that all Adobe products and services are designed from inception with security best practices in mind, the operational security team created the Adobe Operational Security Stack (OSS). The OSS is a consolidated set of tools that help product developers and engineers improve their security posture and reduce risk to both Adobe and our customers while also helping drive Adobe-wide adherence to compliance, privacy, and other governance frameworks.

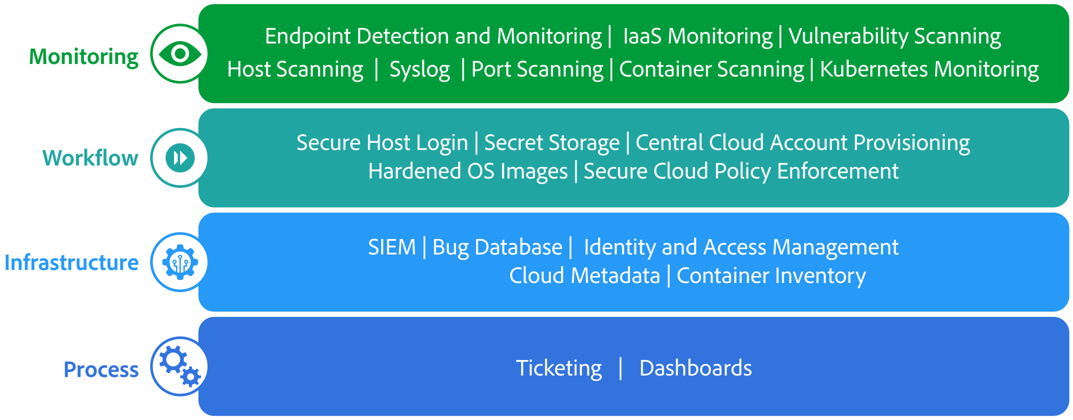

Monitoring
Endpoint Detection and Monitoring | IaaS Monitoring | Vulnerability Scanning
Host Scanning | Syslog | Port Scanning | Container Scanning | Kubernetes Monitoring
Workflow
Secure Host Login | Secret Storage | Central Cloud Account Provisioning
Hardened OS Images | Secure Cloud Policy Enforcement
Infrastructure
SIEM | Bug Database | Identity and Access Management
Cloud Metadata | Container Inventory
Process
Ticketing | Dashboards

Figure 9: The Adobe Operational Security Stack

Adobe maintains several published standards covering our ongoing cloud operations that are available for view upon request. A detailed description of the Adobe OSS and the specific tools used throughout Adobe can be found in the Adobe Operational Security Overview.

Adobe Enterprise Security

In addition to securing our products and services as well as our cloud hosting operations, Adobe also employs a variety of internal security controls to help ensure the security of our internal networks and systems, physical corporate locations, employees, and our customers' data.

More information on our enterprise security controls and standards we have developed for these controls can be found in the Adobe Enterprise Security Overview.

Adobe Compliance

All Adobe products and services adhere to the Adobe Common Controls Framework (CCF), 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. As much as possible, Adobe leverages leading-edge automation processes to alert teams to possible non-compliance situations and help ensure swift mitigation and realignment.

Adobe products and services either meet applicable legal standards or can be used in a way that enables customers to help meet their legal obligations related to the use of service providers. Customers maintain control over their documents, data, and workflows, and can choose how to best comply with local or regional regulations, such as the General Data Protection Regulation (GDPR) in the EU.

Adobe also maintains a compliance training and related standards that are available for review upon request. More information on the Adobe CCF and key certifications can be found in the Adobe Compliance Certifications, Standards, and Regulations List.

Incident Response

Adobe strives to ensure that its risk and vulnerability management, incident response, mitigation, and resolution processes are 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.

We also maintain internal standards for incident response and vulnerability management that are available for view upon request.

More details about Adobe's incident response and notification process are documented in the Adobe Incident Response Program Overview.

Business Continuity and Disaster Recovery

The Adobe Business Continuity and Disaster Recovery (BCDR) Program is composed of the Adobe Corporate Business Continuity Plan (BCP) and product-specific Disaster Recovery (DR) Plans, both of which help ensure the continued availability and delivery of Adobe products and services. Our ISO 22301-certified BCDR Program enhances our ability to respond to, mitigate, and recover from the impacts of unexpected disruptions. More information on the Adobe BCDR Program can be found in the Adobe Business Continuity and Disaster Recovery Program Overview.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe solutions 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 of our customers' data.

For more information on Adobe security, please go to the Adobe Trust Center.

Adobe

12/22