WHITE PAPER

Adobe Identity Management Services

April 2025

Table of contents

Introduction

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

- **Adobe Identity Service** — Handles authentication and validation of 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.
- **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 users to authenticate themselves to their Adobe desktop applications and cloud services.

Figure 1 (below) depicts the interaction of an end-user with the Adobe IMS using named user licensing. In the example, the user has installed Adobe applications on their desktop or mobile device. When a 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.

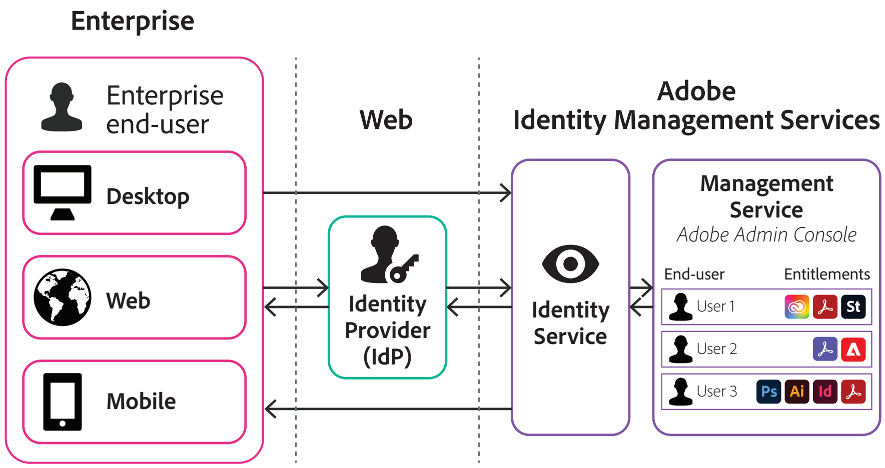

Figure 1: Adobe Identity Management Services Architecture

Based on the user identity type (see next section), Adobe IMS either allows the 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 user's entitlements and completes their requested action. The user can now use the software or services to which they are entitled.

More information about managing users can be found on HelpX.

User Identity Types

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

Enterprise ID is an Adobe-hosted, enterprise-managed option for accounts that are created by administrators of 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 UMAPI. Administrators can set authentication policies for these users, but Adobe fully manages the user's authentication and credentials.

Federated ID is a non-Adobe hosted, enterprise-managed account option in which all identity profiles are provided by a Single Sign-On identity management system and are created, owned, and controlled by the customer's 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 customer organization's identity provider completely controls setting and enforcing authentication policies.

Adobe ID is for Adobe-hosted, user-managed accounts that are created, owned, and controlled by individual users. Adobe performs the authentication, and the user manages the identity. While Adobe supports the use of Adobe IDs in enterprise deployments, we do not recommend it as Adobe ID is better suited for individual or personal use.

Note: Most enterprise organizations use Enterprise or Federated IDs for their employees, contractors, and freelancers, provided their email is within the companies' claimed domains.

For more details, please see HelpX.

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.

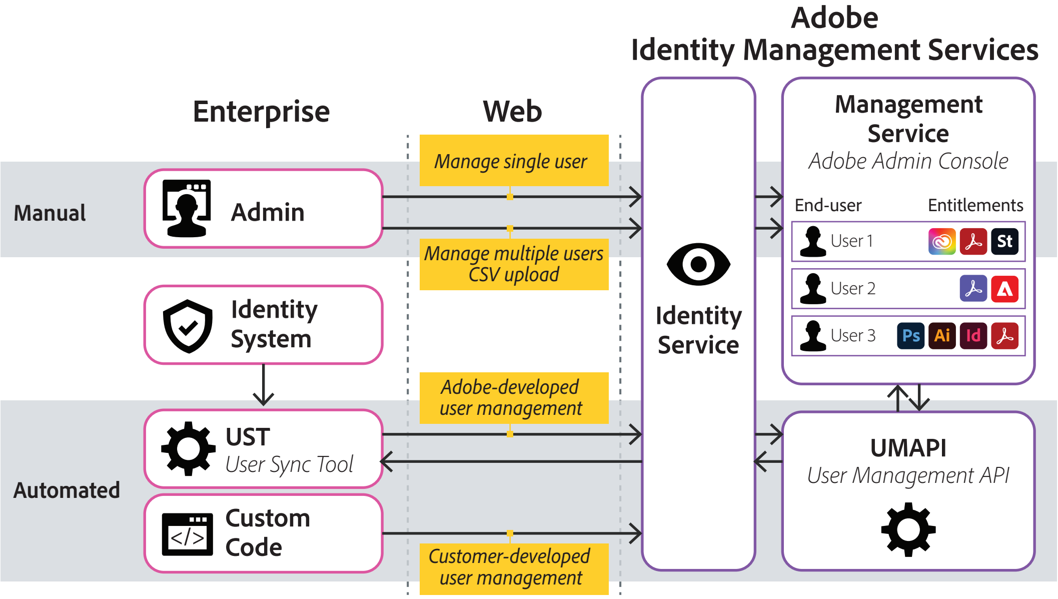

Figure 2: User Identity Management Options

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.

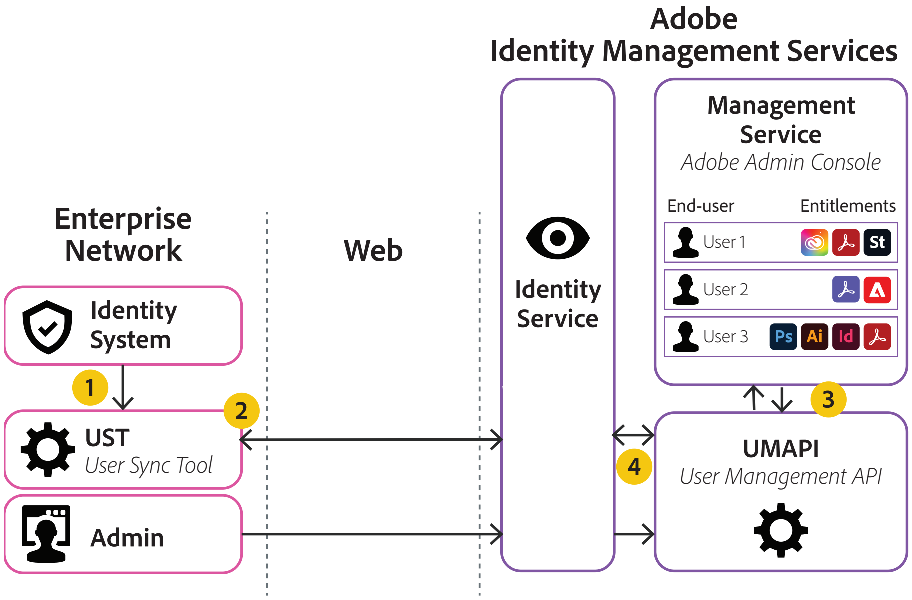

Figure 3: The User Sync Tool (UST)

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.**

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 HelpX.

User Authentication and Authorization Data Flow

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

Interactive authentication and authorization — 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, authorization is designed to occur seamlessly and, to the user, appears as part of the authentication process.

Adobe also supports multi-factor authentication (MFA) after the user has been authenticated using the initial two-step verification in the UI. Adobe offers policies to enforce MFA for Enterprise ID and Adobe ID users. Even when MFA is deployed, authorization occurs seamlessly and, to the user, appears to be part of the authentication process. More information about Adobe's support for MFA can be found on HelpX.

Automated authentication and authorization — After a user has been authenticated using interactive authentication for an initial session, automated authentication utilizes a unique identification token so that the user does not have to log in again for the duration of the session; authorization is designed to occur seamlessly as well. Any time a user interacts with an application or service and is not required to explicitly log in, that 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.

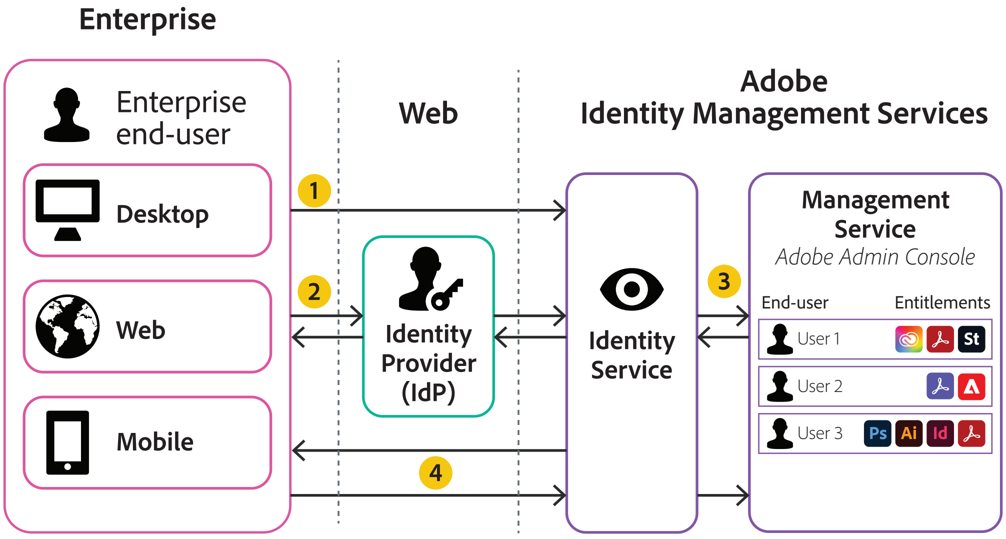

Figure 4: Adobe User Authentication Data Flow

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 user launches a desktop or mobile application or requests access to an Adobe cloud service for the first time. If they are using an Enterprise ID or an Adobe ID, they log in using Adobe IMS.

2. If the user's organization leverages Federated ID, when the 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 user to their identity provider to log in using their corporate credentials.

3. Once the user is properly authenticated, Adobe IMS then conducts the applicable entitlement and policy enforcement checks and redirects the user to the appropriate Adobe cloud service or enables appropriate desktop application licensing.

   As part of this process, Adobe IMS stores a device token on the user's computer or mobile device 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 user's settings. Because the device 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.

4. At this point, the user can concurrently use any Adobe desktop or mobile 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, the access rights are checked based on the user's access token and will be denied.

Adobe offers optional administrative policies that enable enterprise organizations to further limit the lifespan of access tokens by requiring more frequent authentication, which can be useful for certain Adobe Experience Cloud applications. Adobe recommends that customers evaluate and apply these additional policy-based restrictions according to their specific security requirements.

User Identity Data

For further information regarding the identity-related data that Adobe collects, why we collect it, and how it is used, please see the Adobe Privacy Policy.

Conclusion

For more information about Adobe's operational, application, and enterprise security processes, compliance certifications, incident response program, security training and awareness program, and business continuity and disaster recovery program, please see the Adobe Trust Center.