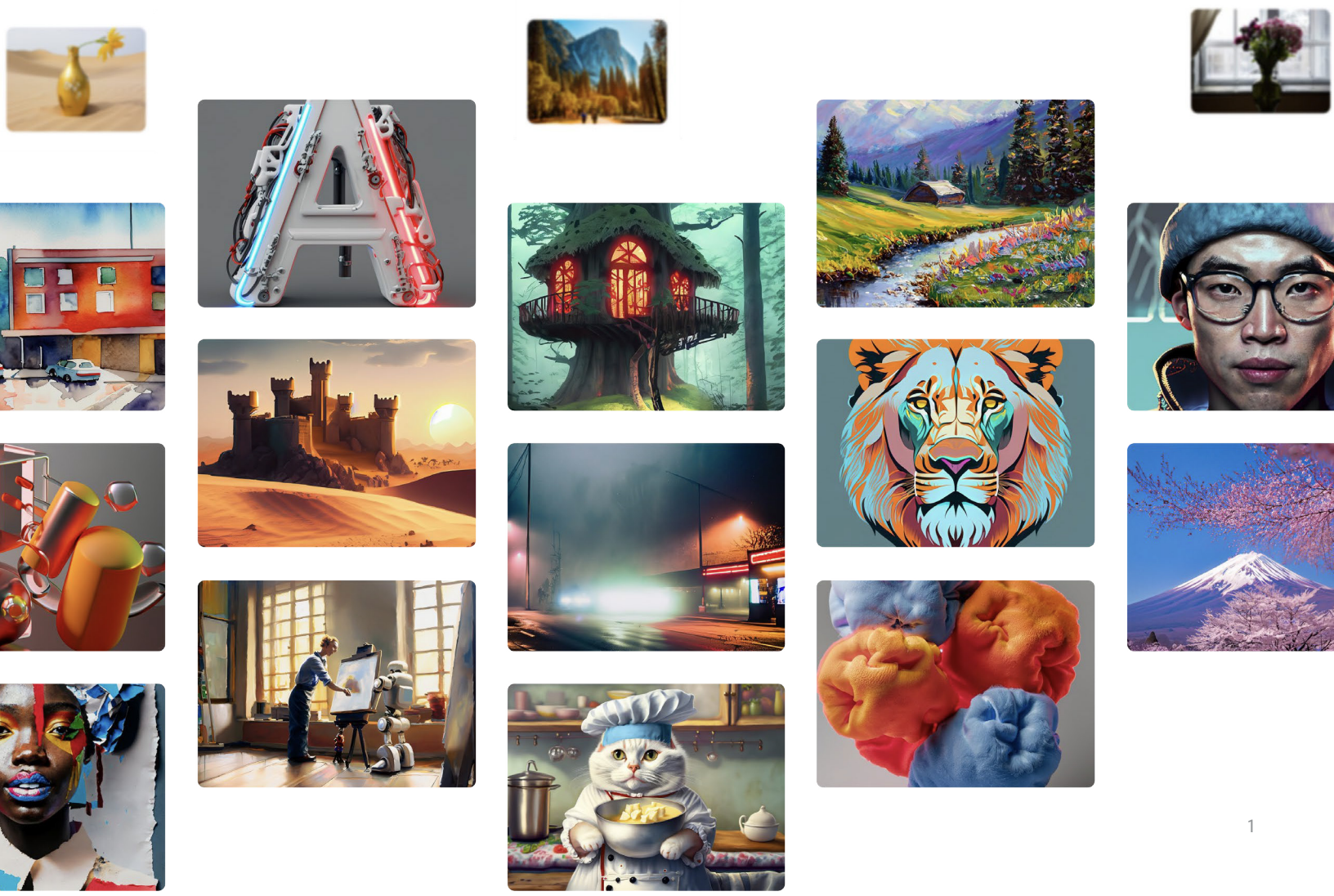
SECURITY FACT SHEET

Adobe Firefly Services

October 2024



About Firefly Services

Firefly Services is a comprehensive set of generative AI and creative APIs that automates workflows. By embedding these capabilities into any production or experience workflow, organizations can scale content generation, editing, and assembly, automating the production of content while maintaining quality and control.

API Families

Firefly Services includes a range of APIs that are grouped into API families:

- **Adobe Firefly APIs** – Automate text-to-image generation for entire images and masked in-painting or expanded out-painting areas. For more information, please see Firefly API.
- **Adobe Photoshop APIs** – Edit and process PSD, JPEG, PNG, and TIFF images using Adobe Photoshop technology. For more information, please see Photoshop API.
- **Adobe Lightroom APIs** – Edit JPEG, PNG, RAW, and other supported file formats using Adobe Lightroom technology. For more information, please see Lightroom API.
- **Content Tagging APIs** – Extract intelligent features from content, organize and streamline content flow, and deliver more impactful, personalized experiences. For more information, please see Content Tagging API.

How to Access Firefly Services

To access Firefly Services APIs, an Adobe Admin must assign the user to the *Developer* role in the organization's Adobe Admin Console, enabling the user to access the Developer Console. The admin must also assign the user a Firefly Services entitlement in the Admin Console, which allows the user to create a project using the Firefly Services APIs and develop applications in the Developer Console.

In the Developer Console, the user can generate an API key (client ID) and client secret. Using these credentials, the user can have any application they create that leverages Firefly Services APIs generate an access token, which is passed along with every API request to validate the application's credentials.

Adobe Identity Management Services (IMS) is used to manage access, including authentication and authorization, to Firefly Services APIs. For more information, please see the Adobe Identity Management Services Security Overview.

API Authentication

Firefly Services support OAuth Server-to-Server credential authentication. For more information, please see the Server to Server authentication documentation.

Firefly Services Architecture and Data Flow

The following example illustrates the data flow between an application built to leverage Firefly Services APIs to generate content in Firefly, edit that content using the Photoshop or Lightroom APIs, and return the content to the application.

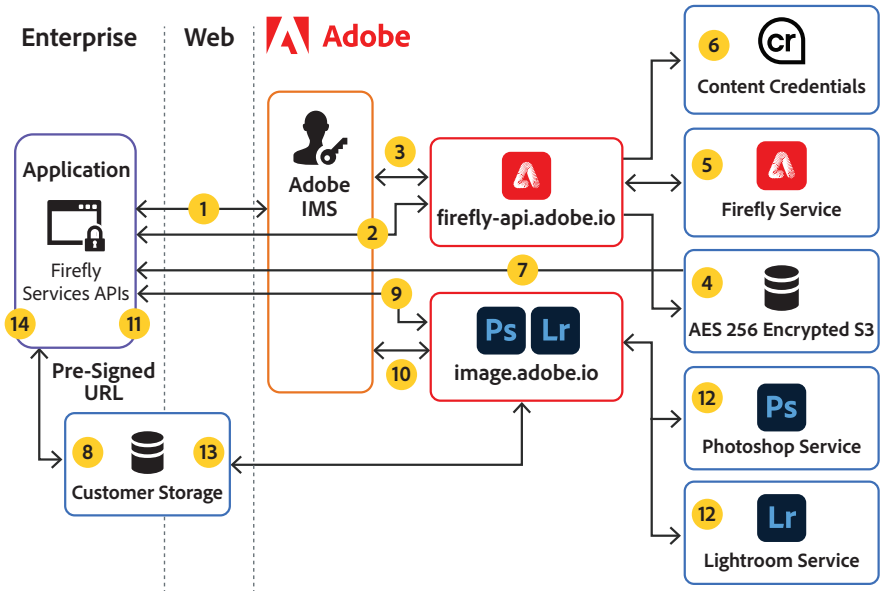


Figure 1: Adobe Firefly Services security architecture and data flow

Data Flow Narrative

Note: All data is encrypted in transit over HTTPS using TLS 1.2 and a minimum of AES 128-bit GCM encryption..

Step 1: The client application requests an access token from Adobe Identity Management Services (IMS) using an API Key (client ID) and client secret.

Step 2: The client application submits an API request to the Firefly API containing the prompt and configuration settings. Note: The Firefly API leverages the Firefly Service for inferencing and generating content. The Adobe Firefly for enterprise (core and web) security fact sheet contains more information about the security posture of Firefly.

Step 3: The Firefly API validates the included API key (client ID) and the access token with Adobe IMS.

Step 4: If the inference process for Firefly requires reference content (e.g., Generative Match, Generative Fill, or Generative Expand), the content is uploaded to an AES 256-bit encrypted AWS S3 storage location and referenced by a pre-signed URL. The reference content is deleted 24 hours after it was initially created.

Step 5: The Firefly Service generates content based on the prompt text, configuration settings and, if utilized, the uploaded reference content. Firefly retrieves any reference content from the pre-signed URL noted in Step 4.

Step 6: The Firefly API attaches a Content Credentials manifest to the generated content and saves this manifest to the Content Credentials cloud.

Step 7: The Firefly API stores the generated content in an AES 256-bit encrypted AWS S3 storage location, generates a pre-signed Firefly URL, and returns the URL to the client application.

Step 8: The client application downloads the generated image from the pre-signed Firefly URL and uploads it to a customer-defined storage location (e.g., Adobe-managed storage, AWS, Azure, Dropbox, or Google Drive).

Step 9: The application submits an API request including the pre-signed URL from Step 8 to the Photoshop/Lightroom API.

Step 10: The Photoshop/Lightroom API validates the included API key (client ID) and the access token with Adobe IMS.

Step 11: The Photoshop/Lightroom API returns a job status link to the client application.

Step 12: The Photoshop/Lightroom API asynchronously performs the requested editing tasks using the relevant application (i.e., either Photoshop or Lightroom). In-process images are cached for the duration of the API transaction.

Step 13: Photoshop or Lightroom stores the completed image in the customer-defined storage location from Step 8.

Step 14: The client application queries the status API via the status link provided in step 11. When Photoshop or Lightroom completes the required processing, the client application downloads the completed asset from customer storage using the pre-signed URL.

Data Encryption

In Transit: All data is encrypted in transit over HTTPS using TLS v1.2 and a minimum of AES 128-bit GCM encryption.

At Rest: If the user chooses Adobe-managed storage as their customer-defined storage location, which is determined on a per-transaction basis, Adobe encrypts the content at rest using AES 256-bit encryption.

Input and Output Content Storage and Processing

Adobe stores input and output information in connection with the services it provides.

Input

By default, Firefly Services store or process the following inputs:

- **Firefly API (firefly-api.adobe.io)**
    - Prompt text input and configuration settings, such as seed values, image styles, tone, depth of field, aspect ratio, etc. (retained for 180 days)
    - A pseudonymous user ID (e.g., i001ad83a-d41f-4afb-9f5c- 7b72c88ae873a) (logged and stored with other data elements as noted)
    - Reference content, if uploaded by the API (cached for 24 hours as described above)
- **Photoshop/Lightroom API (image.adobe.io)**
    - Configuration settings (logged for 30 days)
    - Uploaded images (processed and cached for 24 hours)

Note: Adobe does not include enterprise user content (including Firefly inputs and outputs) in datasets used to train Firefly foundation models. This does not apply to (1) the use of Firefly as part of any feedback or improvement programs in which the customer/user can control the use of their content for training through an opt-in/opt-out menu or (2) the customer's use of any Adobe product or feature that utilizes AI training in order to provide the customer with a service.

Output

By default, Adobe does not permanently store Firefly outputs; instead, they are temporarily cached in application-managed cache storage for 24 hours and can be accessed using a pre-signed URL.

- **Firefly API (firefly-api.adobe.io)**
    - Generated image (stored for 24 hours and accessible via pre-signed URL as described above)
    - A pseudonymous user ID (e.g., i001ad83a-d41f-4afb-9f5c- 7b72c88ae873a) (logged and stored with the other data elements as noted)
    - A cryptographic hash of the image for Content Credentials and stored in the Content Credentials Cloud with the manifest
- **Photoshop/Lightroom API (image.adobe.io)**
    - The processed, masked, or edited image (stored in customer-defined storage as described above)

Content Credentials

Adobe automatically generates Content Credentials for certain Firefly-generated assets to help provide transparency that the asset was created using generative AI.

Content Credentials typically contain the following metadata:

- In certain cases, a thumbnail of the generated image
- The tool/tools used to generate the asset
- Whether the asset was completely generated by Firefly or combined with other content
- A cryptographic hash of the image and its metadata in a verifiable, tamper-evident signature that provides proof that the image and metadata have not been altered. The cryptographic hash is irreversible.

Content Credentials are attached to the exported asset file and stored in the Content Credentials cloud repository, which allows recovery of the Content Credentials in the event it is stripped from the exported asset.

Note: Text prompts are never included in any automatically generated Content Credentials.

User-Generated Content

Firefly Services accept and process user-generated content (UGC). This content is downloaded, secured, and temporarily cached as part of normal service operations as described above.

If the Firefly API workflow includes reference content, it will upload and store that reference content in an AES 256-bit encrypted AWS S3 storage location referenced by a pre-signed URL.

The Photoshop/Lightroom API workflow requires a customer-defined storage location for user-generated content. The API will upload from that location and store processed and edited content into that location via a pre-signed URL.

Hosting Locations

All server-side components of Firefly Services APIs are hosted on Amazon AWS data centers in the US-East-1 (Virginia) and US-West-2 (Oregon) region.

Testing

Adobe teams conduct rigorous testing to reduce the potential for biased and harmful outcomes in our generative AI products. For more information on the development and testing processes for our generative AI solutions, please see the Generative AI Built for Business solution brief.

Questions?

If you have any additional questions about the security posture and capabilities of Adobe Firefly, please contact your Adobe account manager. For all other questions about Adobe's security programs and processes and compliance certifications, please see the Adobe Trust Center.

Adobe