WHITE PAPER

Adobe Workfront Security Overview

September 2024

Table of Contents

Adobe Security

At Adobe, we know the security of your digital experience is important. Security practices are deeply ingrained into our internal software development, operations processes, and tools. Our cross-functional teams strictly follow these practices to help prevent, detect, and respond to incidents in an expedient manner. We keep up to date with the latest threats and vulnerabilities through our collaborative work with partners, leading researchers, security research institutions, and other industry organizations and 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 secure Adobe Workfront and associated data.

About Adobe Workfront

Adobe Workfront is an enterprise work management solution that helps customers manage the entire lifecycle of work in one place. Built for the way people work, the platform is intuitive, flexible, and customizable and provides a 360-degree view of all workplace activities, helping both team members and administration alike to better understand and organize their work.

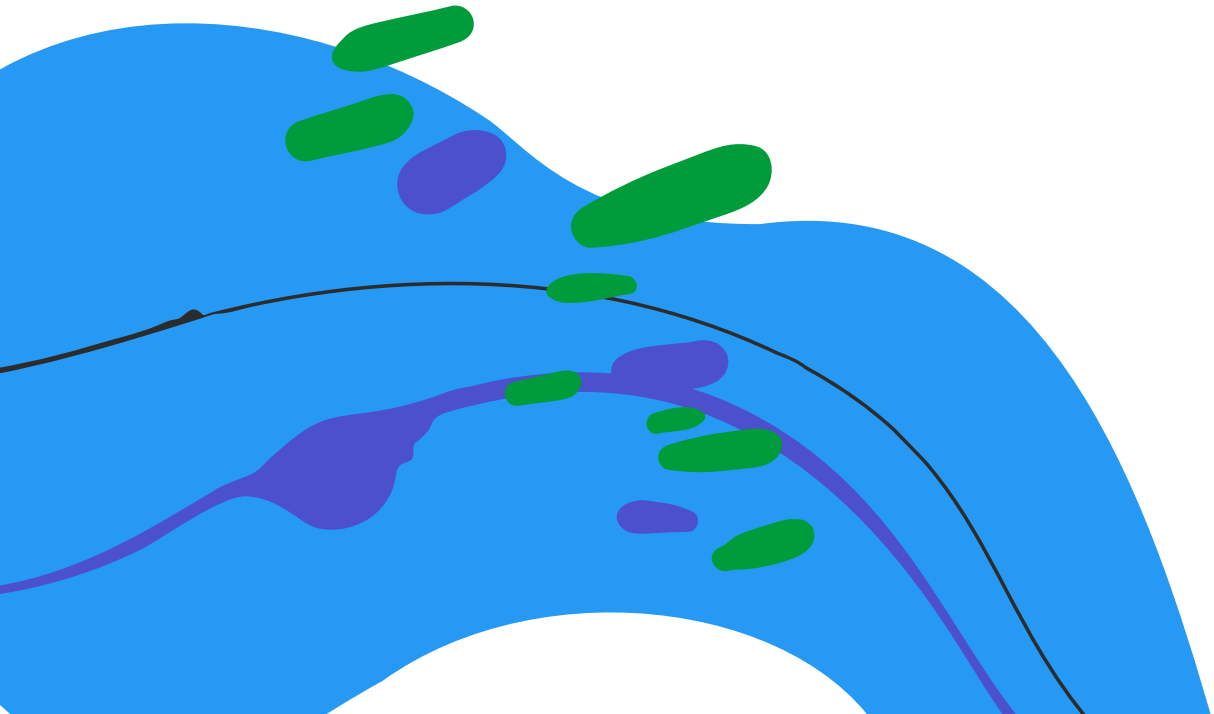
The solution includes the following functionality:

- **Project Management** — Enables planning and executing projects using feature-rich, interactive Gantt charts, real-time reporting, and custom project dashboards and views that give managers complete visibility to manage and bring projects in on-time and on-budget.
- **Reports and Dashboards** — Delivers custom reports and dashboards to unlock the data being tracked in Adobe Workfront. With more than 150 out-of-the-box yet customizable reports and dashboards, customers can change as programs mature and reporting needs grow.
- **Resource Management** — Allows resource managers to make business decisions that ensure the individual workers available today are budgeted against the highest priority work.
- **Team Collaboration** — Empowers teams with front-line conversational information, increasing their acceptance of and participation in the project management process, enabling greater accuracy in projections and more informed decision-making.
- **Time Management** — Allows customers to create and manage timesheets for anyone on the team through a built-in timesheet management portal.

- **Portfolio Management** — Helps prioritize projects and ensure that they are aligned with business goals and requirements.
- **Process Improvement** — Enables organizations to incorporate workflows within the solution, improving communication, coordination, and efficiency.
- **Product Integration** — Integrates seamlessly with a variety of business-critical applications, including turnkey connectors for popular applications.
- **Proofing** – Automatically notifies and updates collaborators and stakeholders on all pending and completed approvals outlined in the project workflow.
- **Auditing and Governance** — Provides a central repository for all project information, enabling the creation of an audit trail to authenticate compliance with corporate standards.

Adobe Workfront also includes three optional add-ons:

- **Workfront Fusion** — Lets customers create, manage, and monitor automated workflows within Workfront and across various third-party applications (Please see the section below for more information on specific security considerations for Workfront Fusion).
- **Workfront Goals** — Helps define, communicate, and achieve strategic outcomes by connecting strategy to work execution and delivery.
- **Workfront Scenario Planner** — Drives speed to execution by enabling the creation of different scenarios to find the optimal plan that delivers on the organizations' overall strategic outcomes.



Solution Architecture

The following diagram describes the components of the Workfront solution and the interconnections between them.

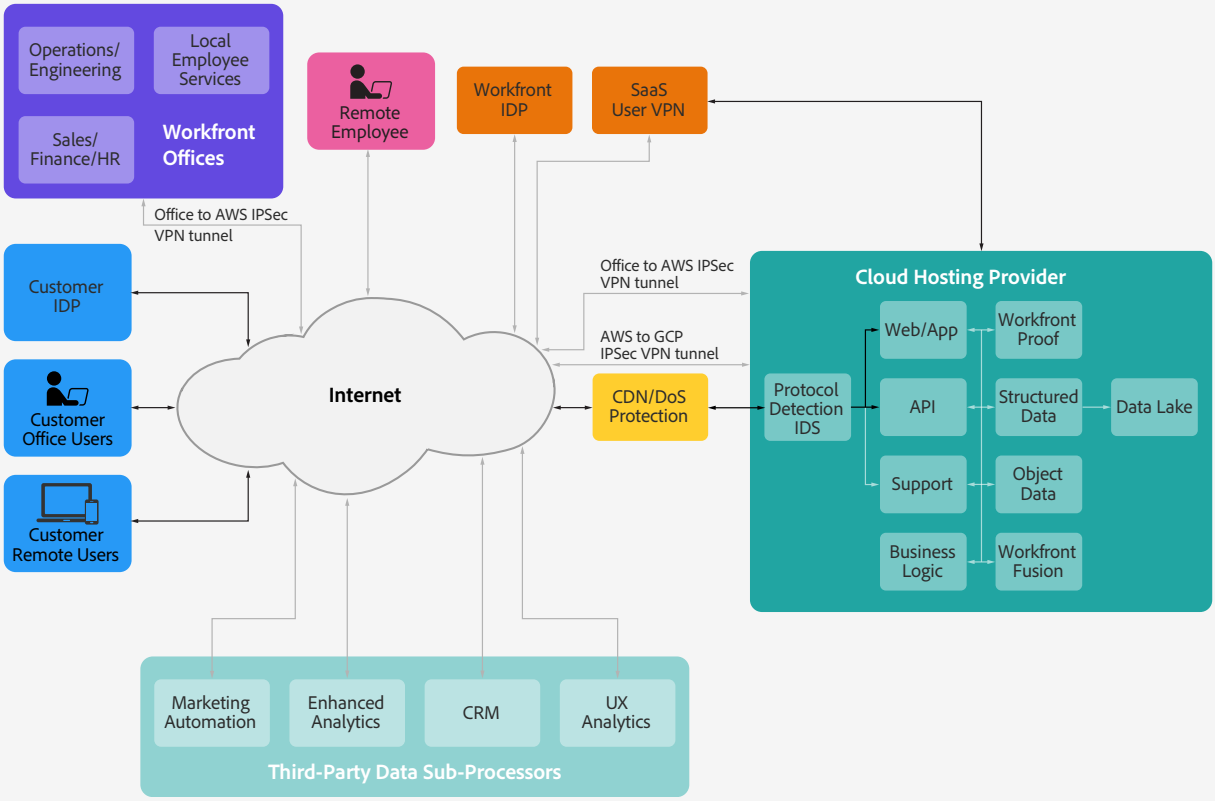


Figure 1: Adobe Workfront Solution Architecture

Security Architecture and Data Flow

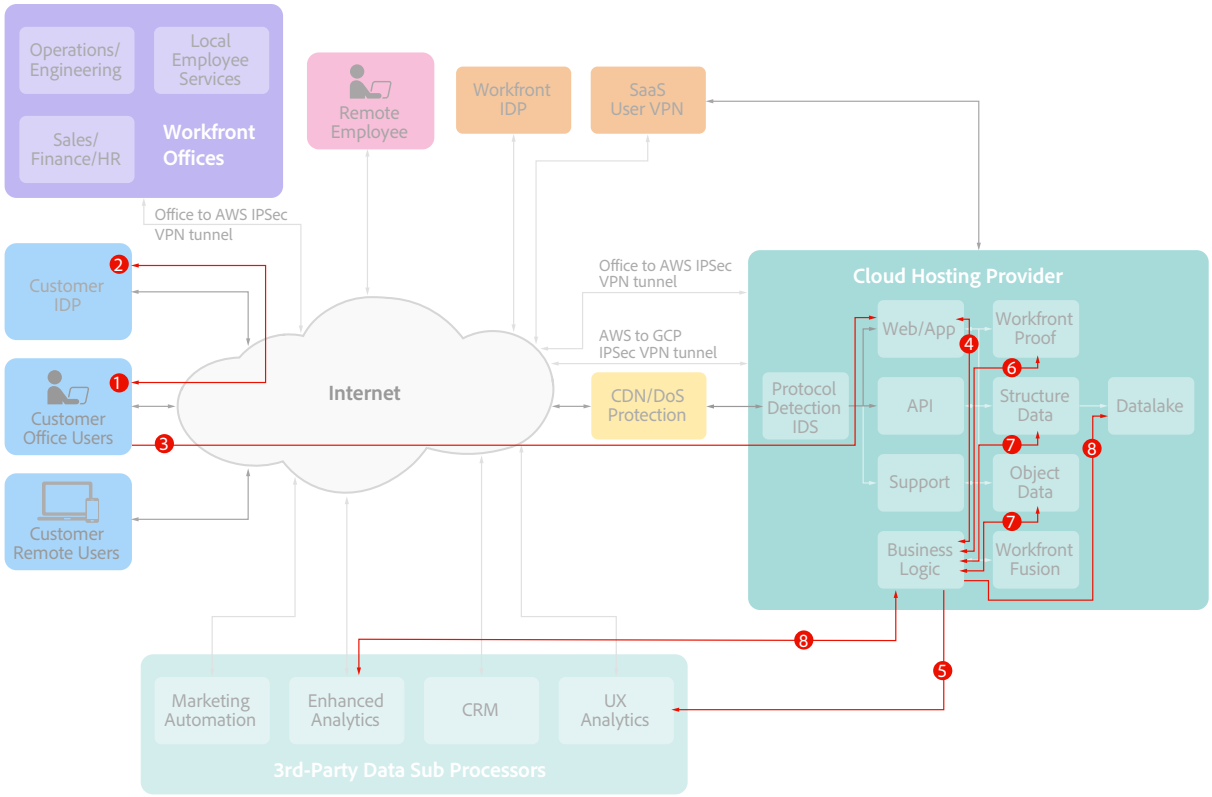


Figure 2: Adobe Workfront Security Architecture and Data Flow

To protect the customer's Workfront URL from downgrade attacks, we implement HTTP Strict Transport Security (HSTS), which only allows access to the website using a secure HTTPS connection. In addition, Workfront protects customers from cross-site request forgery (CSRF/XSRF) and cross-site scripting (XSS) attacks.

Data Flow Narrative

Customers interact with Adobe Workfront in three ways:

- Workfront web UI
- Workfront mobile application
- Workfront API

1. In each case, the connection to Workfront begins with a TLS-1.2-secured HTTP request from the user's web browser to the customer company's Workfront URL.
2. Front-end load balancers and a CDN for static assets receive these HTTP requests and forward them to the Workfront application servers on the cloud hosting provider. Each request is filtered by the native firewall technology employed by the cloud hosting provider, helping ensure that only web requests using TCP port 80 or TCP port 443 are allowed.
3. The Workfront application servers handle the customer-configured authentication mechanisms (SSO, etc.) by initiating a new session or confirming an HTTP request against an existing authorized session.
4. Workfront application servers then route authorized requests between VPCs (virtual private clouds) to connect to Workfront backend databases or pull data from (using authenticated requests) cloud-native storage services.
5. Customers can view the events from these interactions either via the Audit Log (available via the Web UI) or the Event Subscription API.

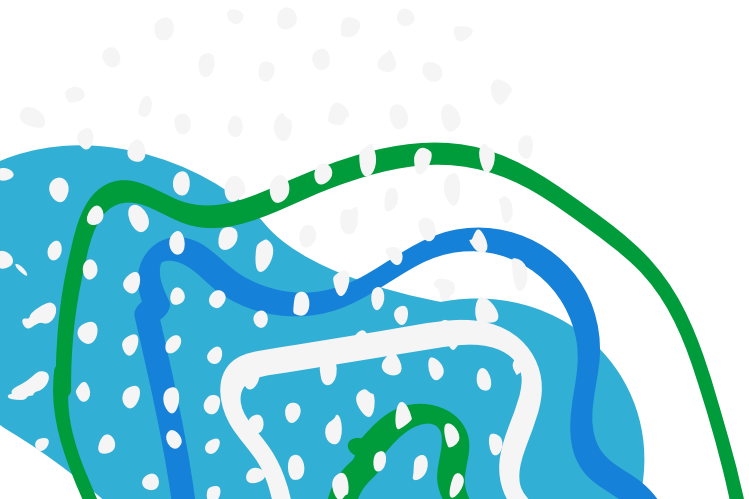
Adobe Workfront uses some third-party data sub-processors to provide certain functionality. A complete list of sub-processors used by Adobe can be found here.

Data Encryption

Adobe Workfront employs PCI DSS approved encryption algorithms to encrypt documents and assets at rest with AES 256-bit encryption and uses HTTPS TLS v1.2 to protect data in transit.

Documents uploaded to Adobe Workfront are stored in cloud-native object storage services. Workfront databases are then encrypted with disk-level encryption technologies.

Workfront utilizes cloud-native key management systems (KMS) to centrally store and manage encryption keys. Workfront encryption keys are generated and stored in a FIPS-140-2 validated (or better) KMS managed by the cloud service provider and are automatically rotated on an annual basis.



User Authentication

Access to Adobe Workfront requires authentication with username and password. We continually work with our development teams to implement new protections based on evolving authentication standards. Users can access Workfront in one of three (3) different types of user-named licensing:

Adobe ID is for Adobe-hosted, user-managed accounts that are created, owned, and controlled by individual users.

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 organization owns and manages the user accounts and all associated assets, Adobe hosts the Enterprise ID and performs authentication. Admins can revoke access to Workfront 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 the customer's IT infrastructure.

Adobe integrates with most SAML2.0 compliant identity providers. Adobe IDs and Enterprise IDs both 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 threats to their security. For Federated ID accounts, Adobe does not manage the users' passwords. More information about Adobe's identity management services can be found in the Adobe Identity Management Services security overview.

API Authentication

Adobe Workfront provides a REST API interface that enables customers to integrate Workfront into their other corporate applications and services. The Adobe Workfront API interface offers three (3) different authentication mechanisms:

1. **Username + Password (+ Digital Certificate)** — The user must supply a valid username and password in order to access the Adobe Workfront API interface. For additional security, users can be required to supply a digital certificate in addition to username + password. Typically, this method of authentication is only used to:
    a. Generate a session token (sessionID) for pre-authenticating future API calls
    b. Generate an API key
    c. Retrieve an API key

2. **Session Token** — The user presents a short-lived session token with each API call. Obtained using one of the two username + password authentication mechanisms mentioned above, the sessionID may be supplied as a URL parameter or in the HTTP header. Customers can configure sessionID lifetime based on their requirements.

3. **API Key** – Only available to users with system administrator-level privileges, the user supplies a valid API key to access the Adobe Workfront API interface. API keys are securely managed and generated within the Workfront application. Customers can configure these keys to automatically expire after a pre-determined amount of time to compel periodic API key rotation. API key expiration can also be configured to expire whenever the corresponding user's password expires. System administrators can revoke all users' API keys if needed.

Administrative Security Controls

Role-Based Access Controls — Workfront includes six (6) out-of-the-box access levels, which are geared toward users with various roles in the organization. The access level the user is assigned to in their user profile governs their rights and privileges in Workfront. By default, a user's access level affects which areas are visible to that user in the Global Navigation Bar. System administrators also can copy canned access levels and modify them to add/remove functionality.

IP Allowlists — In some cases, administrators must add certain IP addresses to their firewall's or mail server's allowlist in order to allow open communication between their environment and Adobe Workfront.

Administrators also have access to a variety of other system security preferences in Workfront. Changes made to these security preferences impact all users of the Workfront solution. Therefore, Adobe recommends that customers configure their system security preferences during initial implementation and only revisit them when absolutely necessary.

For more information on role-based access controls, IP allowlists, and specific security preferences available for Workfront, please visit Adobe Workfront One.

Hosting Locations & Security

Adobe Workfront is hosted in data centers around the world managed by trusted and certified Adobe cloud hosting partners in the U.S. (Oregon, California, Iowa, and Virginia) and Europe (Ireland and Germany).The specific data center region or location is determined by the customer's location, e.g., if the customer is based in the United States, their Workfront solution will be hosted in a data center located in the U.S. Similarly, if the customer is based in the E.U., their Workfront solution will be hosted in a data center in the E.U.

Figure 3: Adobe Workfront Hosting Locations

About Adobe Workfront Fusion

Adobe Workfront Fusion enables customers to create, manage, and monitor automated workflows within Workfront and across various third-party applications. With Workfront Fusion, data and information flow freely – yet securely – across systems and teams, increasing productivity and efficiency with a single, connected solution.

Solution Architecture

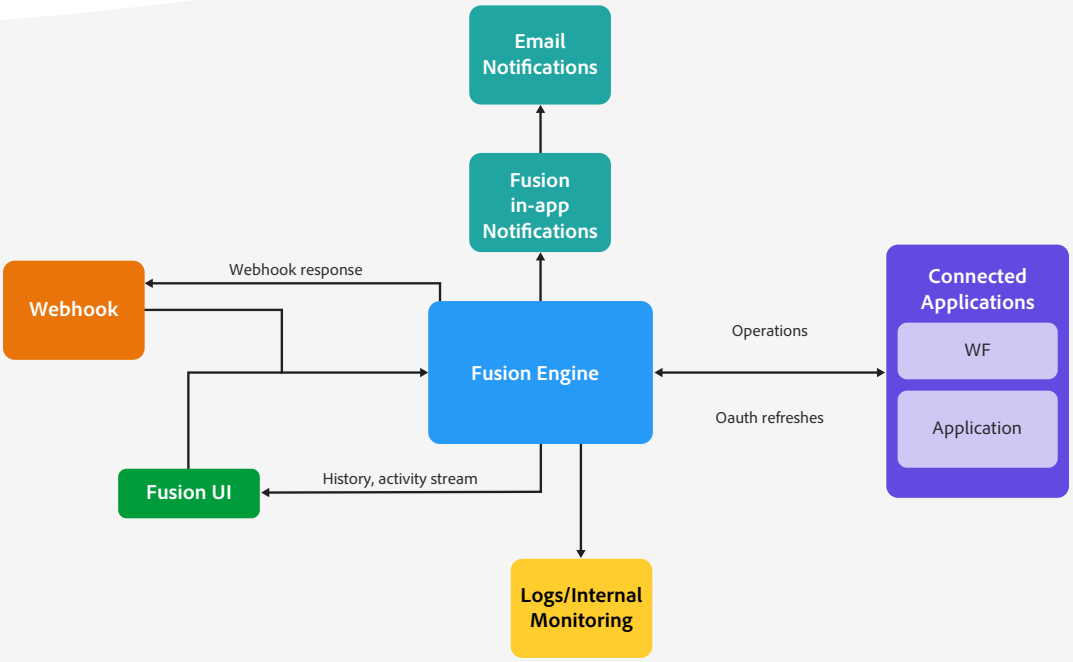


Figure 4: Adobe Workfront Fusion Solution Architecture

Data Flow

Customers create and edit automation use cases called scenarios using the Fusion visual designer. A scenario is comprised of a series of modules that perform operations, including interactions with connected applications and data transformation. A Fusion module interacts with a web service via its API; The module defines what action is performed.

The Fusion engine executes scenarios based on trigger events. Scenarios with instant triggers are based on data received from another application. Scheduled scenarios are processed according to a schedule set using the Fusion designer.

During execution, Fusion sends data to and receives data from other systems. The Fusion engine also streams data to the Fusion user interface so that the user can view data that is currently being processed or that has already been processed, which can be accessed in Fusion's execution history.

Each connection between the user's browser and Workfront Fusion is encrypted using HTTPS TLS 1.2. Fusion also refreshes OAuth connections that support reauthorization.

Administrative Security Controls

Workfront Fusion provides administrators the same security controls as Workfront, which can be found above in the Workfront section of this document. For more information on role-based access controls, IP allowlists, and specific security preferences available for Workfront, please visit Adobe Workfront One.

Workfront Fusion Connectors

Workfront Fusion includes a pre-built set of application connectors that enable administrators to connect to other applications. For more information on how to add these connectors, please go to Adobe Workfront One.

Workfront Fusion also includes a set of universal connectors that enable administrators to connect to other applications for which a pre-built standard connector does not exist. These universal connectors support OAuth 2.0 Authorization Code Flow, Basic Authentication, and other forms of authentication based upon the specific needs of the target application.

In cases where an OAuth 2.0 Authorization Code Flow cannot be used, Workfront Fusion must store authentication credentials for the third-party application. Workfront Fusion uses cryptographically secure hash algorithms (AES encryption (PBKDF2-SHA512) to encrypt credentials.

Regardless of the method of authentication used, once credentials for a third-party application are entered into Workfront Fusion, those credentials are never visible to any subsequent user, including the user that entered them originally.

All data between Workfront Fusion and connected third-party solutions is encrypted in transit using TLS 1.2. Mutual TLS is available for use in the HTTP connector.

Questions?

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.

09/24