WHITE PAPER

Adobe Acrobat with Acrobat Services Security Overview

August 2025

Adobe

Table of contents

About Adobe Acrobat with Acrobat Services

Adobe Acrobat and Acrobat Services, along with Adobe Acrobat Sign and Adobe Acrobat AI Assistant, comprise Adobe's Document Cloud solution. Document Cloud enables organizations to build smarter document workflows and store files in the Adobe Document Cloud infrastructure. Using Adobe Acrobat with Acrobat Services, customers can turn virtually any content into an electronic document that is easily shared with others and can automate the generation, manipulation, and transformation of PDF files from any supported surface.

For information about the security posture of Adobe Acrobat Sign, please see the Adobe Acrobat Sign security overview. For information about the security posture of Acrobat AI Assistant, please see the Adobe Acrobat AI Assistant security fact sheet.

Acrobat User Experiences

Users can access Adobe Acrobat through a variety of surfaces:

- **Acrobat Pro** — Desktop application for laptop and desktop users
- **Acrobat online** — Web application within supported browsers on desktop and mobile devices, including Chrome, Microsoft Edge, Firefox, and Safari
- **Acrobat Reader mobile client** — Free downloadable application from the Apple App Store and Google Play for mobile and tablet users

Adobe Acrobat is also integrated into several Microsoft productivity tools. The security posture for each integration is detailed in the "Adobe Acrobat Microsoft Integrations" section below.

Adobe Acrobat Services

Acrobat Services include the following:

- Send PDF — Send a PDF to a recipient using an email client
- Organize PDF — Insert, delete, reorder, or rotate pages in a PDF
- Create PDF — Convert a Word, Excel, and PowerPoint document, as well as images or photos, into a PDF file
- Export PDF — Convert a PDF into an editable Microsoft Word, Excel, PowerPoint, or RTF file
- Edit PDF — Edit an existing PDF on a mobile device or laptop

- Combine PDF — Combine multiple files into a single PDF and assemble document packages from anywhere
- Fill & Sign — Complete a form and add a signature
- Adobe Scan — Capture and convert anything into a searchable, high-quality PDF

Acrobat Document Security

Redaction

Adobe Acrobat Pro includes a set of redaction tools that help customers protect sensitive or confidential information, including permanent deletion of both text and graphic images in a document before distribution. In addition, users can search and redact based on patterns, such as phone numbers, credit card numbers, and email addresses. The information selected is completely removed from the file, not just masked as with other tools or methods. Using the document sanitization feature, customers can also remove hidden information and non-graphic objects, such as metadata that may be present in the PDF.

File Sharing

PDF files created with Adobe Acrobat stored in Document Cloud are automatically labeled "Private," which means the content is only visible to the user who uploaded it. To share a document with another individual or group of individuals, the user must specifically share the link to the URL of the document to the recipient(s).

Users may share files as "view only" or "review." If the user sends the link with the view only restriction, the recipient will receive the document with read-only functionality. Alternatively, if the user sends the document for review, the recipient may comment on the document, but they may not edit or alter it in any way. Links may be sent to recipients via email, text, or any collaboration software.

Asset Settings and Sharing Restrictions

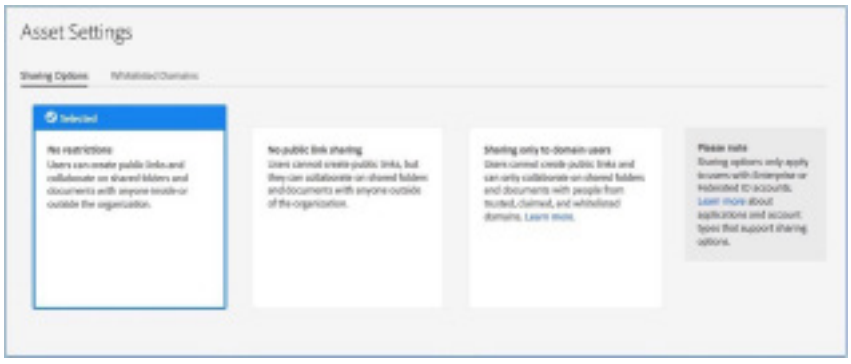

Figure 1: Acrobat Services Asset Settings

Content stored in Document Cloud can also have sharing restrictions enabled through the Asset Settings feature in the Adobe Admin Console. This feature allows the customer organization's Adobe administrator to turn off public link sharing as well as limit the Adobe Document Cloud review service to only the enterprise-claimed domain and any other allowed domains. When sharing restrictions are enabled, recipients must sign in. If the customer's Adobe admin turns on "Sharing only to domain users" mode, users can only share content with other users within their organization; external sharing is completely disabled.

Microsoft Purview Information Protection

Microsoft Purview Information Protection (MPIP) is a Microsoft rights management solution. Users of Azure Information Protection and other Microsoft Purview Information Protection solutions can use Acrobat or Acrobat Reader to read labeled and protected content. The most current desktop versions of Acrobat Pro and Acrobat Standard can natively apply and edit MPIP sensitivity labels and policies to their PDF files without a plug-in or separate installation.

Operating System-level Mitigations

Adobe Acrobat enables key operating system-level mitigations that make it more difficult for attackers to exploit Acrobat for nefarious purposes, including Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), security cookies (canaries), Control-Flow Guard (CFG), and Library Loading Protections.

Sandboxing

Sandboxing is a highly respected security method that creates a confined execution environment in which to run programs with low rights or privileges. Sandboxes help protect users' systems from being harmed by untrusted documents that contain executable code. In the context of Acrobat, untrusted content is any PDF file and the processes that it invokes. Acrobat treats all PDF files as potentially corrupt and confines all processing that the PDF file invokes to the sandbox.

Protected Mode

Enabled by default whenever a user launches Acrobat, Protected Mode is Adobe's implementation of sandboxing technology that limits the level of access granted to the application, safeguarding systems running Microsoft Windows from malicious PDF files that might attempt to write to or read from the computer's file system, delete files, or otherwise modify system information. In Acrobat, Protected Mode not only protects against attackers that attempt to install malware on a computer system but also block malicious individuals from accessing and extracting sensitive data and intellectual property from the corporate network. On Microsoft Windows, Protected Mode can run in isolation in an AppContainer. For information about Protected Mode on MacOS, please see Enhanced Security Settings.

Protected View

Protected View extends the security of Acrobat beyond blocking write-based attacks to also include read-based attacks that attempt to steal sensitive data or intellectual property via PDF files. Protected View assumes that all PDF files are potentially malicious and confines processing to the sandbox unless the user specifically indicates that a file is trusted. Because Protected View confines the execution of untrusted programs (e.g., any PDF file and the processes that it invokes) to a sandbox, malicious code embedded in a PDF cannot write to or read from a computer's file system.

Protected View is supported in both scenarios in which users open PDF documents — within the standalone Acrobat application and within a browser. Protected View on Windows 8 and later always runs in an AppContainer, which provides an even stronger locked-down environment. When a user opens a potentially malicious file within Protected View, Acrobat displays a yellow message bar (YMB) at the top of the viewing window. The YMB indicates that the file is untrusted and reminds the user that they are in Protected View, thereby disabling many Acrobat features and limiting user interaction with the file. Essentially, the file is in "read-only" mode and Protected View prevents embedded or tag-along malicious content from tampering with the system.

To trust the file and enable all Acrobat features, the user can click the "Enable All Features" button in the YMB. This action exits Protected View and provides permanent trust for the file by adding it to Acrobat's list of privileged locations. Each subsequent opening of the trusted PDF file from the same location disables Protected View provisions.

Acrobat Services Security

User Authentication

Administrators entitle end-user access to Acrobat Services by utilizing named user licensing in the Adobe Admin Console. For more information about these identity types and Adobe Identity Management Services, please see the Adobe Identity Management Services security overview.

Document and User-Generated Content Storage

Acrobat Services leverage multi-tenant storage. User-generated content and documents are stored redundantly in multiple data centers and on multiple devices in each data center. All network traffic undergoes systematic data verification and checksum calculations to prevent corruption and help ensure integrity. Finally, stored content is replicated synchronously and automatically to other data center facilities within that customer's region so that data integrity is maintained even with the loss of data in two locations.

User-generated content and documents uploaded to Document Cloud are stored in the regional data center that corresponds to the country code associated with the user uploading the data, regardless of identity type. For more information, please see Document Cloud Data Centers.

Administrators can allocate individual cloud storage for some Enterprise ID and Federated ID accounts through the Adobe Admin Console, but they do not have direct access to any of the user's documents or content stored in Acrobat Services storage. However, admins can assume ownership for the user's account as well as revoke access. Deleting these types of accounts with existing shared services storage renders any data in cloud storage inaccessible to the user and that user's data will be deleted after 28 days. For more information, please see Adobe storage for business.

Data Encryption

By default, Acrobat Services user-generated content and documents are encrypted in transit with HTTPS TLS 1.2 encryption. Acrobat Services content is encrypted at-rest using AES 256-bit symmetric security keys that are unique to each customer and each customer's claimed domain. These encryption methods apply to both permanent and temporary document storage.

Dedicated Encryption Keys

In addition to standard, built-in encryption capabilities, administrators can add another layer of control and security for documents at-rest with a dedicated encryption key for some or all the domains in the customer organization. Acrobat Services content can then be encrypted at-rest using that dedicated encryption key, and, if required, the encryption key can be revoked from the Admin Console. Revoking the key will render all content encrypted with that key inaccessible to all end users and will prevent both content uploads and downloads until the encryption key is re-enabled.

Note: Only Adobe Document Cloud files can be encrypted using the dedicated encryption key; metadata cannot be encrypted. More information on managing encryption using a dedicated key can be found on the Manage encryption page.

Electronic and Digital Signatures

Using Adobe Acrobat with Acrobat Services, users can use different tools to work with signatures, including:

- **Fill & Sign tool** — Lets users open a PDF, fill in form fields, and sign the document electronically.
- **Certificates tool** — Enables users to sign documents with an e-signature backed by a digital certificate that is cryptographically bound to the signature field. Each digital certificate (or digital ID) uniquely identifies the signer and is issued by a trust service provider (TSP) or certificate authority (CA) listed on the Adobe Approved Trust List (AATL) or the European Union Trusted Lists (EUTL). The Certificates tool also allows users to add timestamps to documents and certify documents with a tamper-evident seal.

Acrobat Microsoft Integrations

Adobe partners with Microsoft to integrate Acrobat with their productivity tools, which enables Acrobat with Acrobat Services to be accessed natively from within Microsoft SharePoint and OneDrive, Microsoft Teams, and Microsoft Word, Excel, and PowerPoint. Users can also access Acrobat from a browser extension to Microsoft Edge on Windows.

Conclusion

For more information about Adobe security, including our enterprise, product, and operational security processes, security testing program, compliance and certifications, incident response program, and business continuity and disaster recovery (BCDR) processes, please see the Adobe Trust Center.