Acrobat DC security overview

The world's leading PDF solution for creating, editing, and managing documents

Table of contents

When you trust your business's information to a third-party application, security is critical. Adobe has more than 20 years of leadership in secure digital documents, and pioneered the standard for PDF and digital signatures. Hundreds of thousands of organizations have produced billions of PDFs worldwide because they trust Adobe Acrobat software and Adobe PDF to help them prepare, protect, and share their most critical documents every day.

Adobe Acrobat DC with Adobe Document Cloud services is the complete PDF solution for today's mobile, connected world. It combines Acrobat desktop software with the Adobe Acrobat Reader mobile app enhanced with premium mobile features and Document Cloud services to help organizations build smarter document workflows and meet end-user demand for mobile solutions while ensuring document security across devices. With Acrobat DC, you'll always stay up to date with access to the latest security updates and the latest features that can be deployed on your schedule.

This document covers Adobe's comprehensive approach to security as it relates to Acrobat DC—spanning document, application, and cloud security—to help protect your information and experience even further.

Document security

Document authors can use Acrobat DC software to create PDF documents and apply a host of security measures, including encryption, access control, certificate signatures, and permanent removal of text and images via redaction tools. The convenience of using the Actions functionality in Acrobat DC to define a set of security tasks that users can easily apply without formal training or special tools makes it easy for organizations to keep information private and confidential.

Encryption

Security standards supported by Acrobat DC:

- 256-bit Advanced Encryption Standard (AES)
- Standards supported by the European Telecommunications Standards Institute (ETSI)

Access control

Share documents with confidence by easily applying passwords and permissions to control access or prevent changes to any PDF document, restrict printing, copying, or altering the document.

Electronic and digital signatures

In Acrobat DC, users can choose between two different tools to work securely with signatures: Send for Signature and Certificates.

Send for Signature lets users manage end-to-end signing processes that comply with *e-signature* laws in the United States, the European Union, and most industrialized nations worldwide. With it, they can request signatures from others, track the signing process, and archive signed documents and audit trails automatically. The entire process is managed securely, and documents and audit trails are certified by Adobe with a tamper-evident seal. Send for Signature is powered by *Adobe Sign*, an *Adobe Document*

Cloud solution, which is independently certified to meet rigorous security standards, including ISO 27001, SOC 2 Type 2, and HIPAA, as well as PCI DSS.

The Certificates tool lets you sign documents with certificate-based digital IDs from trusted service providers on the Adobe Approved Trust List (AATL), or the European Union Trusted Lists (EUTL). Signing with a certificate ID issued by a trusted third-party certificate authority is one of the most secure methods of signing documents electronically. The ID is uniquely linked to, and capable of identifying, the signer. The signer's certificate is cryptographically bound to the document during the signing step using the private key uniquely held by that signer. Acrobat DC validates their signature—and the authenticity of the document they signed—by connecting automatically with the certificate authority for verification. This type of signature complies with PDF electronic signature standards, including PDF Advanced Electronic Signature (PAdES) Parts 2, 3, and 4 as well as the U.S. Department of Defense Joint Interoperability Test Command (JITC) usage of cryptography and PKI with AES-256/RSA-4096/SHA-512. The Certificates tool also lets you add timestamps to documents, and certify them with a tamper-evident seal.

To learn more about electronic and digital signatures, read the *Transform business processes with electronic and digital signature solutions* white paper.

True redaction

Acrobat DC offers a set of redaction tools that help you protect sensitive or confidential information. You can permanently delete both text and graphic images in a document before you distribute it. You can even search and redact based on patterns, such as phone numbers, credit card numbers, and email addresses. The information you select is completely removed from the file, not just masked as with other tools or methods.

With the Sanitize Document feature, remove hidden information and non-graphic objects such as metadata that may be present in the PDF.

Application security

The improved security features in Acrobat DC help provide protection against attacks that attempt to exploit the PDF file format to install malware on your system and/or extract sensitive data from your system.

At Adobe, security practices are deeply ingrained into our culture, software development, as well as engineering processes. Acrobat DC and Acrobat Reader are engineered using industry standard security practices—for access management, data confidentiality, and document integrity—to help protect your documents, data, and personal information.

Secure engineering

Adobe DC applications are engineered using the Adobe Secure Product Lifecycle (SPLC) process, which includes several hundred rigorous security activities spanning software development practices, processes, and tools. The Adobe SPLC is integrated into several stages of the Acrobat DC product lifecycle, from design and development to quality assurance, testing, and deployment. For additional information about Adobe security processes, community engagement, and the Adobe SPLC, see *www.adobe.com/security*.

Protected Mode in Adobe Acrobat Reader DC

To protect you and your organization from malicious code that attempts to use the PDF format to write to or read from a computer's file system, Adobe delivers a cutting-edge implementation of sandboxing technology called Protected Mode, which was introduced in Adobe Reader X.

In Acrobat Reader DC, Protected Mode extends the protection against attackers who attempt to install malware on your computer system to include blocking malicious individuals from accessing and extracting sensitive data and intellectual property from your computer or corporate network.

Protected Mode is enabled by default whenever you launch Acrobat Reader DC. It limits the level of access granted to the program, 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. Reader Protected Mode (on Windows 8.1 and above) can now run in an AppContainer. To learn more about AppContainer: *https://msdn.microsoft.com/en-us/library/windows/desktop/mt595898(v=vs.85).aspx*.

In addition, as part of the company's ongoing efforts to integrate security into multiple stages of the product lifecycle through the SPLC process, Adobe conducts regular reviews of existing code and hardens it as appropriate, further improving application security and enhancing the safety of your data when you use Adobe products.

Protected View in Acrobat DC

What is sandboxing?

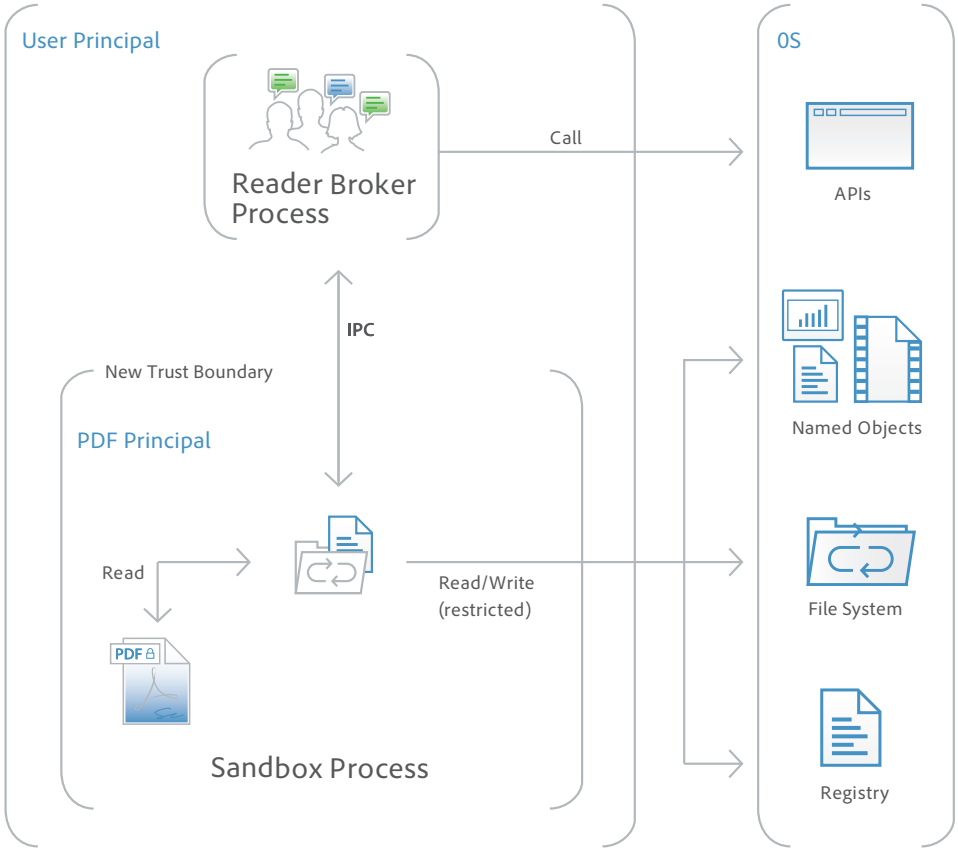
Sandboxing is a highly respected method by security professionals that creates a confined execution environment for running programs with low rights or privileges. Sandboxes help protect users' systems from being harmed by untrusted documents that contain executable code. In the context of Acrobat Reader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

Similar to Protected Mode in Acrobat Reader DC, Protected View is an implementation of sandboxing technology for the rich Acrobat DC feature set. In Acrobat DC, Adobe extends the functionality of Protected View beyond blocking write-based attacks that attempt to execute malicious code on your computer system using the PDF file format to read-based attacks that attempt to steal your sensitive data or intellectual property via PDF files.

Like Protected Mode, Protected View confines the execution of untrusted programs (for example, any PDF file and the processes that it invokes) to a restricted sandbox to avoid malicious code using the PDF format from writing to or reading from your computer's file system.

Protected View assumes that all PDF files are potentially malicious and confines processing to the sandbox, unless you specifically indicate that a file is trusted. Protected View is supported in both scenarios in which users open PDF documents—within the standalone Acrobat DC application and within a browser. Protected View on Windows 8 and above always runs in an AppContainer. This provides an even stronger locked-down environment for customers who enable Protected View.

When you open a potentially malicious file within Protected View, Acrobat DC displays a yellow message bar (YMB) at the top of the viewing window. The YMB indicates that the file is untrusted and reminds you that you are in Protected View, thereby disabling many Acrobat DC 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 your system. To trust the file and enable all Acrobat DC features, you 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 disables Protected View restrictions.



JavaScript execution

Acrobat DC offers sophisticated and granular controls for whitelisting and blacklisting JavaScript execution across a variety of environments such as Microsoft Windows and Macintosh. The Adobe JavaScript Whitelist Framework selectively enables JavaScript for specific PDF files, sites, hosts, or documents that have been signed using a trusted certificate. Additionally, the Adobe JavaScript

Whitelist Framework
Selectively enable JavaScript for your trusted workflows by whitelisting documents using privileged locations, which allows trust to be granted based on Microsoft Windows security zones, certified documents, or by adding specific files, folders, or hosts.

Blacklist Framework allows you to use JavaScript as a part of business workflows while protecting users and systems from attacks that target specific JavaScript API calls. By adding a specific JavaScript API call to the blacklist, you can block it from executing without completely disabling JavaScript. You can also prevent individual users from overriding your decision to block a specific JavaScript API call, helping to protect your entire enterprise from malicious code.

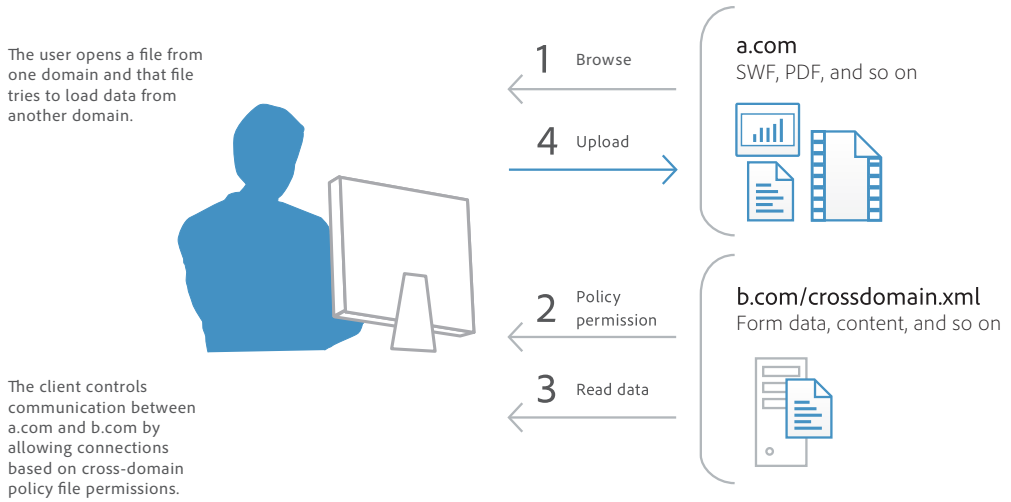
Cross-domain configuration

By default, Acrobat DC disables unrestricted cross-domain access for both Windows and Mac OS X clients, preventing attackers from exploiting rich PDF files to access resources in another domain.

By leveraging the built-in support for server-based, cross-domain policy files, you can allow Acrobat DC and Acrobat Reader DC to handle data across domains. This cross-domain policy file—an XML document—is hosted on the remote domain, granting access to the source domain and allowing Acrobat DC or Acrobat Reader DC to continue the transaction.

You want to enable Adobe cross-domain support for the following scenarios:

- You need selective cross-domain access and want to leverage other features, such as recognition based on a digital certificate.
- You want to centrally manage cross-domain access permissions from a single, server-based location.
- You need to implement workflows that include data requests from multiple domains for returning form data, SOAP requests, references to streaming media, and .NET HTTP requests.



User-friendly security alerts

In addition to Adobe incident response processes and security alerts, Acrobat DC implements a user-friendly method of security alerts through the YMB. When enhanced security is enabled and the PDF file is not set as a privileged or trusted location, the YMB appears when a PDF file tries to execute a potentially risky action such as:

- Invoke cross-domain access
- Run privileged JavaScript
- Invoke a JavaScript-invoked URL
- Call a blacklisted JavaScript API
- Inject data
- Inject scripts
- Play embedded legacy multimedia

In Acrobat DC and Reader DC, the YMB appears at the top of the document with the warning or error message. The user can choose to trust the document once or always. Choosing always adds the document to the application's list of privileged documents.

The Options button allows users to set trust on the fly, once, or always. You can also preconfigure trust enterprise-wide for files, folders, and hosts so that the YMB never appears in a trusted enterprise workflow.

Cloud security

Adobe is constantly monitoring and improving our cloud services, systems, and processes to help customers meet the growing demands and challenges of securing and protecting data. Document Cloud services, including Adobe Sign and PDF services used by Acrobat DC, are designed to help ensure the confidentiality, integrity, and availability of your documents. Document Cloud services are compliant with ISO 27001, PCI DSS, and SOC 2 Type 2, and meet many additional industry-specific compliance certifications, standards, and regulations. For additional information on our approach to cloud security, please see the *Adobe Document Cloud Security Overview*.

Data center security

Today, the Document Cloud data center that hosts PDF services and file storage resides in an American National Standards Institute (ANSI) tier-4 data center managed by our trusted cloud service provider, Amazon Web Services (AWS). AWS maintains very strict controls around data center access, fault tolerance, environmental controls, and security. Only approved, authorized Adobe employees, cloud service provider employees, and contractors with a legitimate, documented business are allowed access to the secured site in Virginia, U.S. For additional information on AWS data center security please see *https://aws.amazon.com/security/*.

Data encryption and privacy

Adobe products and services, including Document Cloud services, are designed with privacy in mind. Document Cloud encrypts documents and assets at rest using the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) 256-bit encryption and supports Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security (TLS) to ensure that data in transit is also adequately protected.

Document Cloud employees and trusted vendors only access customer data to perform certain business and support functions, or as required by law. Adobe does not provide any government with direct or systematic access to customer data that we store. For more information about Adobe's privacy policies please see *www.adobe.com/privacy*.

Integration with operating system architectures

Always-on security

To provide an additional layer of defense against attacks that attempt to control desktop systems or corrupt memory, Acrobat DC takes advantage of built-in, always-on security protections in the Windows and Mac OS X operating systems.

Data Execution Prevention (DEP) restricts the placement of data or dangerous code into memory locations that are defined as protected by the Windows operating system. Apple offers similar protection for Mac OS X Lion, including Stack DEP and Heap-based DEP, and extends this protection to 32-bit and 64-bit apps, making all applications more resistant to attack.

Address space layout randomization (ASLR) hides memory and page file locations of system components, making it difficult for attackers to find and target those components. Both Windows and Mac OS X Lion use ASLR. In Mac OS X Lion, ASLR is extended to 32-bit and 64-bit apps.

Registry-level and plist configuration

Acrobat DC gives you a variety of tools to manage security settings, including registry-level (Windows) and plist (Mac OS) preferences. With these settings, you can configure clients, pre- and post-deployment, to do the following:

- Turn enhanced security on or off
- Turn privileged locations on or off

- Specify predefined privileged locations
- Lock certain features and disable the application UI so that end users cannot change the settings
- Disable, enable, or configure almost any other security-related feature

Easier deployment and administration

Software security hardening

Security enhancements, such as Protected View, are just one example of the extensive engineering investments Adobe has made in hardening Acrobat DC against threats. By making the software more robust against attacks, Adobe can reduce or even eliminate the need for out-of-band security updates and lower the urgency of regularly scheduled updates. All of this increases operational flexibility and decreases Total Cost of Ownership (TCO), particularly in large environments with high security-assurance requirements.

Support for Citrix and application virtualization

With named user licensing support for Citrix XenApp, Citrix XenDesktop, VMware Horizon, and Microsoft App-V, you can deliver secure remote access to the Acrobat functionality your users need.

Support for Enterprise Mobility Management (EMM) solutions

Adobe is committed to helping enterprise customers meet demand for mobile business productivity solutions while safeguarding enterprise security and compliance. The Acrobat Reader and Adobe Sign mobile apps both support the Android for Work EMM platform, and Adobe Acrobat Reader for Microsoft Intune is available for iOS and Android. Acrobat Reader also supports the AppConfig platform. Learn more about *IT resources*.

Support for Windows Server Group Policy Objects and Microsoft Active Directory

Windows Server Group Policy Objects (GPO) and Microsoft Active Directory enable you to automate one-to-many management of computer systems. Adobe has added support for certified Microsoft Active Directory Administrative (ADM) templates for Group Policy in Acrobat DC, allowing you to provide on-demand software installation and automatic repair of applications. When you need to further configure applications after deployment, you can use ADM templates to propagate the requisite settings across your organization.

Support for Microsoft SCCM and SCUP

With Acrobat DC, you can efficiently import and publish updates via Microsoft System Center Configuration Manager (SCCM) to ensure that your managed Windows desktops are always current with the latest security patches and updates.

Support for Microsoft System Center Updates Publisher (SCUP) catalogs enables you to automate updates to your Acrobat DC software across your organization as well as streamline initial software deployments. SCUP can automatically import any update issued by Adobe as soon as it is available, making it easier and more efficient to update your Acrobat DC deployments. Integration with SCCM and SCUP helps reduce the TCO of your Adobe software, because you can roll out patches organization-wide easier and faster.

Support for Apple Package Installer and Apple Remote Desktop

In Acrobat DC, Adobe has implemented the standard Apple Package Installer provided by Mac OS X rather than the proprietary Adobe Installer. This makes it easier to deploy Acrobat software to Macintosh desktops in the enterprise, because you can now use the Apple Remote Desktop management software to manage your initial software deployment and subsequent upgrades and patches from a central location.

Cumulative, regularly scheduled updates and patches

To help you keep your software up to date, Adobe proactively delivers regularly scheduled updates that contain both feature upgrades and security fixes. For rapid responses to zero-day attacks, Adobe delivers out-of-cycle patches as needed. Adobe leverages cumulative patching as much as possible to reduce the effort and cost required to keep systems up to date. Adobe also aggressively tests security patches before release to help ensure compatibility with existing installations and workflows.

The date of each planned update is pre-announced on the Adobe Product Security Incident Response Team (PSIRT) blog at *blogs.adobe.com/psirt*.

To view the latest security bulletins and advisories about Adobe products, visit *www.adobe.com/support/security*. For more detailed information on Adobe products and security features, visit the Adobe Security library at *www.adobe.com/go/learn_acr_appsecurity_en*.

Adobe Customization Wizard and Enterprise Toolkit

For greater control over your enterprise-wide deployments, Adobe provides these tools:

- **Adobe Customization Wizard**—Free, downloadable utility that enables you to customize the Acrobat installer and configure application features prior to deployment.
- **Adobe Enterprise Toolkit (ETK) for Acrobat and Windows**—Auto-updating, customizable application that contains the Adobe Preference Reference. The Adobe ETK also includes a growing list of resources of interest to enterprise administrators.

Learn more about these tools at *IT resources*.

Conclusion

With Acrobat DC, Adobe takes the security of PDF documents and your data to a whole new level. From extended application security to help protect against the theft of your sensitive corporate data and intellectual property as well as block installation of dangerous malware on your computer systems to integration with additional tools that make administering enterprise-wide deployments easier than ever before, Acrobat DC delivers greater levels of security at a lower TCO than any prior version of Acrobat DC.

For more information
Solution details:
www.adobe.com/security

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

6/17