

Taking PDF security to a new level with Adobe Reader[®] and Adobe Acrobat[®]

Acrobat X family of products raises the bar

Table of contents

- 1: Improved application security
- 4: Tighter Integration with operating system architectures
- 4: Reduced total cost of ownership
- 5: Easier deployment and administration
- 5: Content security
- 6: Conclusion

Adobe Reader X and Adobe Acrobat X take the security of PDF documents—and your data—to a whole new level. Engineered with security in mind, Adobe Reader X and Adobe Acrobat X deliver better application security, thanks to cutting-edge ‘sandboxing’ technology, as well as more granular controls, tighter integration with both the Microsoft[®] Windows[®] and Apple Mac OS X operating system architectures, streamlined patching features, and improved tools for deployment and administration. The new features in Adobe Reader X and Adobe Acrobat X enable users to experience reduced total cost of ownership (TCO) over previous versions of the Adobe Reader X and Adobe Acrobat X products.

In addition, the Adobe Secure Software Engineering Team (ASSET) and the Adobe Product Security Incident Response Team (PSIRT) work together to help ensure that your data is safe and secure when you use Adobe products. Supplementing our internal security efforts, Adobe’s involvement in the Microsoft Active Protections Program (MAPP) ensures the advance sharing of product vulnerability information with security software providers, such as antivirus and intrusion detection and prevention vendors, so the industry can work together to reduce the risk of vulnerabilities in Adobe Acrobat X and Adobe Reader X.

The new security features in Adobe Reader X and Adobe Acrobat X help reduce the risk posed by PDF-based malware.

Improved application security

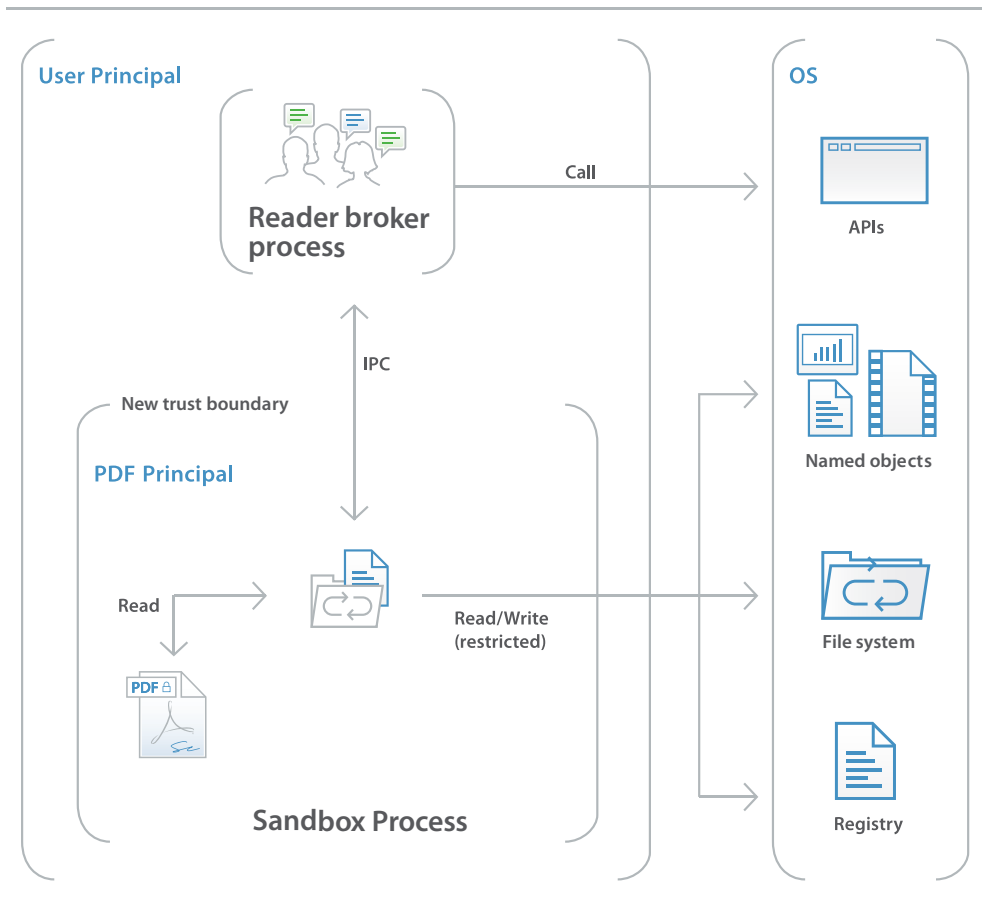
Protected mode in Adobe Reader X

To protect you and your organization from malicious code that attempts to use the PDF format to write to a computer’s file system, Adobe provides Protected Mode, an implementation of ‘sandboxing’ technology.

Enabled by default whenever you launch Adobe Reader X, Protected Mode helps prevent attackers from installing malware on a user’s system, thereby reducing the risk of potential security threats. Specifically, Protected Mode limits the level of access granted to the program, safeguarding systems running the Microsoft Windows operating system from malicious PDF files that may attempt to write to the computer’s file system, delete files, or otherwise modify system information.

What is 'sandboxing'?

Highly respected by security professionals, sandboxing is a method of creating a confined execution environment for running programs with low rights or privileges. Sandboxes protect users' systems from being harmed by untrusted documents that contain executable code. In the context of Adobe Reader, the untrusted content is any PDF and the processes it invokes. Adobe Reader X treats all PDFs as potentially corrupt and confines all processing the PDF invokes to the sandbox.



In addition, as part of the company's ongoing efforts to integrate security into every stage of the product lifecycle through the Adobe Secure Product Lifecycle (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 Adobe Acrobat X

Similar to Protected Mode in Adobe Reader, Protected View is an implementation of sandboxing technology for the rich Adobe Acrobat feature set and is available in Acrobat X, Version 10.1. Just like Protected Mode, Protected View confines the execution of untrusted programs (e.g., any PDF file and the processes it invokes) to a restricted sandbox to avoid malicious code using the PDF format from writing to your computer's file system.

Protected View assumes all PDF files are potentially malicious and confines processing to the sandbox unless you specifically indicate that a file is trusted. While Protected View is supported in both scenarios in which users open PDF documents—within the standalone Adobe Acrobat X application and within a browser—the user experience in each scenario is slightly different.

In the standalone Adobe Acrobat X application, Acrobat displays a Yellow Message Bar (YMB) at the top of the viewing window when you open a potentially malicious file within Protected View. This bar indicates that the file is untrusted and reminds you that you 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 any embedded or tag-along malicious content from tampering with your system. To trust the file and enable all Adobe Acrobat X features, you can click on the "Enable All Features" button in the YMB and Adobe Acrobat will exit Protected View, providing permanent trust for the file by adding the file to Acrobat's list of privileged locations. Every subsequent opening of the trusted PDF disables Protected View restrictions.

When you open a PDF file within a browser, Protected View provides a streamlined experience that does not require a Yellow Message Bar. Instead, all Adobe Reader features are available within the browser environment, as well as the features that are enabled when a document author uses Acrobat to extend features to Reader users—including signing existing form fields, adding new signature fields, saving form data, etc.

Adobe JavaScript controls

You can also use the Adobe JavaScript controls to:

- Turn the JavaScript engine on or off
- Enable or disable JavaScript-invoked URLs
- Control the execution of high-privileged JavaScript independent of other permissions
- Enable high-privileged JavaScript in certified documents

Adobe gives you the flexibility to selectively bypass these restrictions for trusted locations, including files, folders, and hosts.

JavaScript execution

The Adobe Acrobat X family of products offers sophisticated and granular controls for managing JavaScript execution in both Windows and Mac OS X environments. The Adobe JavaScript Blacklist Framework allows JavaScript to be used 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. In Windows environments, the blacklist is maintained in the Windows registry; in Mac OS X environments it is stored in the Mac OS X FeatureLockdown file.

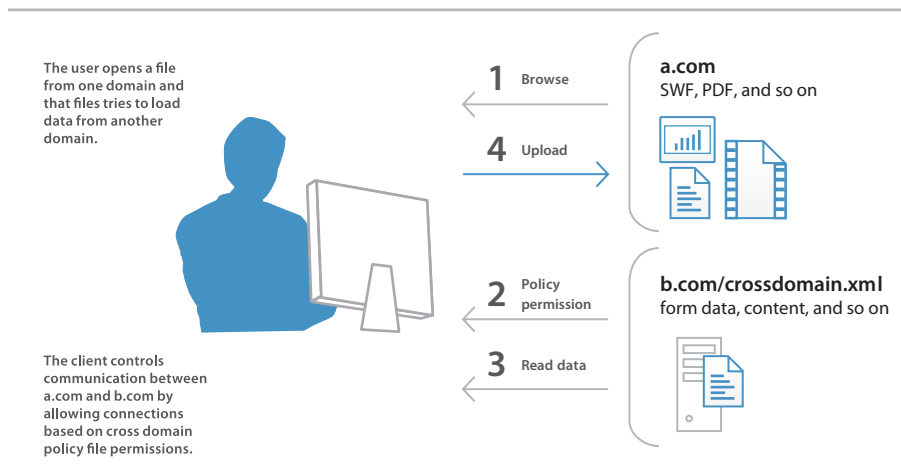
Cross-domain configuration

By default, the Adobe Acrobat X family of products disable unrestricted cross-domain access for both Microsoft 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 Adobe Acrobat X and Adobe Reader X 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 Adobe Acrobat X or Adobe Reader X to continue the transaction.

You'll want to enable Adobe cross-domain support when you:

- Need selective cross-domain access and want to leverage other features, such as recognition based on a digital certificate;
- Want to centrally manage cross domain access permissions from a single, server-based location;
- 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

The Adobe Acrobat X family implements a user-friendly method of security alerts through a non-intrusive Yellow Message Bar (YMB). The YMB replaces traditional dialog boxes that obscure content on the page, making it easier for the user to view and respond to the alert.

In Adobe Acrobat X or Adobe Reader X client, 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.

When enhanced security is enabled and the PDF is not already set as a privileged (e.g., trusted) location, the YMB appears when a PDF tries to execute a potentially risky action, including:

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

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

Tighter integration with operating system architectures

Always-on security

Providing an additional layer of defense against attacks that attempt to control desktop systems or corrupt memory, the Adobe Acrobat X family of products take advantage of built-in, always-on security protections in the Microsoft Windows and Mac OS X operating systems.

- Data Execution Prevention (DEP) prevents placement of data or dangerous code into memory locations that are defined as "protected" by the Windows operating system. Apple offers similar executables protection for Mac OS X 10.6 in the 64-bit Safari browser.
- 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 10.6 use ASLR.

Registry-level and plist configuration

The Adobe Acrobat X family of products give you a variety of tools to manage security settings, including registry-level (Windows) and plist (Macintosh) preferences. With these settings, you can configure clients, both pre- and post-deployment, to:

- 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, and otherwise configure almost any other security-related feature

Reduced total cost of ownership

Software security hardening

Security enhancements like Adobe Reader Protected Mode and Acrobat Protected View are just two examples of the extensive engineering investments Adobe has made in hardening the Acrobat product family against current and emerging threats. By making the software more robust against attack attempts, 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 TCO, particularly in large environments with high security assurance requirements.

Support for Microsoft SCCM/SCUP

With the Adobe Acrobat X family of products, 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.

New support for Microsoft System Center Updates Publisher (SCUP) catalogs enables you to automate updates to your Adobe Acrobat X and Adobe Reader X 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, thereby making it easier and more efficient to update your Adobe Acrobat X and Adobe Reader X deployments. New integration with SCCM/SCUP helps reduce the TCO of your Adobe software, because patches can be rolled out organization-wide, simpler and faster.

Support for Apple Package Installer and Apple Remote Desktop

In the Adobe Acrobat X family of products, 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 Adobe Acrobat and Acrobat Reader 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.

Easier deployment and administration

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 also leverages cumulative patching as much as possible to reduce the effort and cost required to keep systems up-to-date and aggressively tests security patches before release to help ensure compatibility with existing installations and workflows.

Adobe also offers the following security websites and notification services:

To view the latest security bulletins and advisories about Adobe products, please visit www.adobe.com/support/security/

You can see the latest security incident reports and vulnerability fixes on the Adobe PSIRT blog at blogs.adobe.com/psirt/

For more detailed information on Adobe products and security features, please visit the Adobe Security Library at www.adobe.com/go/learn_acr_appsecurity_en

Adobe Customization Wizard and AIM

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

- Adobe Customization Wizard—A free, downloadable utility that enables you to customize the Acrobat Installer and configure application features prior to deployment;
- Administrator's Information Manager (AIM)—An auto-updating, customizable Adobe AIR® application that contains the Preference Reference. AIM also includes a growing list of other resources of interest to enterprise administrators.

Content security

Beyond application security, Adobe supports an array of industry-standard mechanisms to help secure and authenticate the information stored in your PDF documents, including digital signatures, rights management, and document best practices.

Digital signatures

Digital signatures save time and money compared to “wet” signatures, and they help document authors and recipients ensure the integrity and authenticity of a document's contents. With Adobe Reader X and Adobe Acrobat X, you can easily add a standards-based digital signature to a document, check that signature for validity, and add permissions and restrictions to control the signature workflow.

Rights management

The Adobe Acrobat X family of products works with Adobe LiveCycle® Rights Management ES2 software to deliver rights management capabilities that enable you to protect confidential data or other sensitive information from leaking outside your organization or getting into the wrong hands. With it, you can control access, printing, copying, and editing at the document, user, or group level, and dynamically change those policies throughout the lifetime of the document. Plus, because anyone with Adobe Reader can securely access this content, protected documents are easy to view and do not require the recipient to purchase or download additional products or plug-ins.

Consistent best practices

The new Action Wizard feature in Adobe Acrobat X lets you easily script document processes and deploy them across the organization, helping to ensure that all users are following best practices when preparing and protecting public-facing documents.

Managing sensitive information

Users can consistently and quickly remove sensitive information from files using one-button sanitization and enhanced redaction tools. Powerful, standards-based encryption technologies allow end users to set passwords and permissions to control access or prevent changes to any PDF document.

Conclusion

With the Adobe Acrobat X family of products, Adobe takes the security of PDF documents and your data to a new level. From improved application security and more granular controls to tighter operating system integration, Adobe Acrobat X and Adobe Reader X are engineered with security in mind. Adobe Reader X and Adobe Acrobat X users experience greatly reduced TCO over previous versions of the Adobe Reader and Adobe Acrobat products due to better application security, tighter OS integration, streamlined patching features, and improved tools for deployment and administration.

Plus, Adobe Acrobat X and Adobe Reader X are backed by the Adobe team of product security experts, the Adobe Secure Software Engineering Team (ASSET). Working together with the Adobe Product Security Incident Response Team (PSIRT), ASSET helps ensure that your data is safe and secure whenever you use Adobe products.

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

Adobe, the Adobe logo, Acrobat, Adobe AIR, AIR, LiveCycle, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Apple, Mac OS, and Macintosh are trademarks of Apple Inc., registered in the U.S. and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2011 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

05/11