PDF security reaches new levels with Adobe® Reader® XI and Adobe Acrobat® XI

Acrobat XI Family of products raises the bar again

Table of contents

Adobe Reader XI and Adobe Acrobat XI continue to take the security of PDF documents—and your data—to an entirely new level. As with previous versions of the Adobe Acrobat family of products, both Reader XI and Acrobat XI are engineered with security in mind, delivering improved application security and more granular user-level and administrator-level security controls to provide protection against today's increasing number of advanced persistent threats (APTs) that attempt to steal intellectual property electronically from organizations. In addition, tighter operating system integration and easier deployment and administration tools deliver the lowest total cost of ownership (TCO) of any prior version of Reader and Acrobat.

The Adobe Secure Software Engineering Team (ASSET) and the Adobe Product Security Incident Response Team (PSIRT) work tightly together to help ensure that your data is safe and secure when you use Adobe products. In addition, 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 that the industry can work together to reduce the risk of vulnerabilities in Acrobat XI and Reader XI.

Improved application security

The improved security features in Reader XI and Acrobat XI provide protection against attacks that attempt to exploit the PDF file format to:

- Install malware on your system
- Extract sensitive data from your system

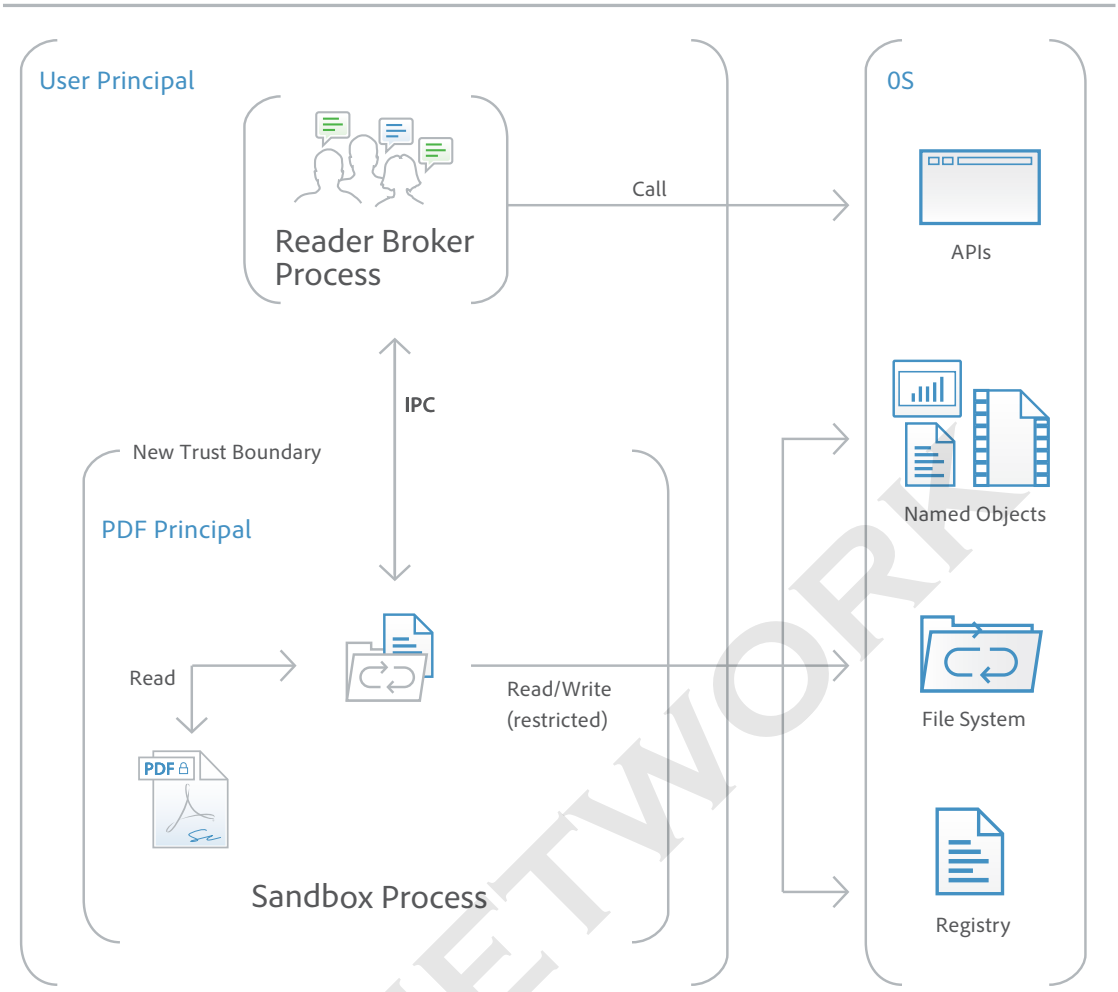
Protected Mode in Reader XI

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 Adobe Reader XI, 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 Reader XI. It limits the level of access granted to the program, safeguarding systems running 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.

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 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 file and the processes that it invokes. Reader XI treats all PDF files as potentially corrupt and confines all processing that the PDF file 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 Acrobat XI

Similar to Protected Mode in Adobe Reader, Protected View is an implementation of sandboxing technology for the rich Adobe Acrobat feature set. In Acrobat XI, 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 XI application and within a browser.

When you open 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 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 embedded or tag-along malicious content from tampering with your system. To trust the file and enable all Acrobat XI 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.

Whitelist Framework
Selectively enable JavaScript for your trusted workflows by whitelisting documents using Privileged Locations, which allows trust to be granted based on WinOS Security Zones, Certified Documents, or by adding specific files, folders, or hosts.

JavaScript execution

The Acrobat XI Family of products offers sophisticated and granular controls for whitelisting and blacklisting JavaScript execution in Windows and Mac OS X environments.

In Adobe Reader XI, you can use the Adobe JavaScript Whitelist Framework to selectively enable JavaScript for specific PDF files, sites, hosts, or documents that have been signed using a trusted certificate in Windows and Mac OS X environments. The new Privileged Locations feature in Adobe Reader XI also allows you to grant trust based on WinOS Security Zones, Certified Documents, or by adding specific files, folders, or hosts, so you can enable JavaScript in your trusted workflows.

The Adobe JavaScript 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. 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.

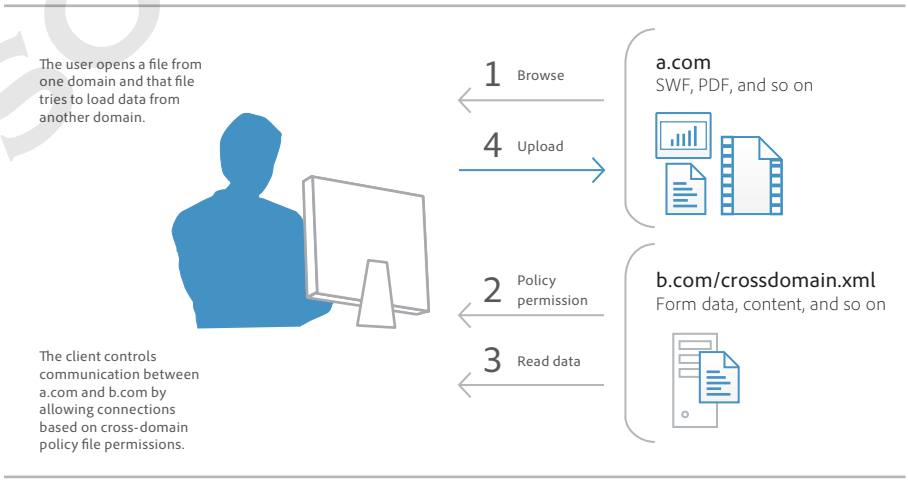
Cross-domain configuration

By default, the Acrobat XI Family of products 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 XI and Reader XI 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 XI or Reader XI 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

The Acrobat XI Family implements a user-friendly method of security alerts through the nonintrusive 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 Acrobat XI and Reader XI, 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 file is not already set as a privileged or trusted location, the YMB appears when a PDF files tries to execute a potentially risky action, including the following:

- 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

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.

Tighter 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, the Acrobat XI Family of products takes advantage of built-in, always-on security protections in the Windows and Mac OS X operating systems.

Data Execution Prevention (DEP) prevents the 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 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

The Acrobat XI Family of products 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 for reduced total cost of ownership

Software security hardening

Security enhancements, such as Protected Mode and Protected View, are just two examples of the extensive engineering investments Adobe has made in hardening Reader and Acrobat 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 Citrix and application virtualization

With new support for Citrix XenApp 6.0 and 6.5 and Windows Terminal Server on Windows Server® 2008, you can deploy Acrobat XI and Reader XI in virtual environments.

Support for Adobe Reader and Acrobat Multilingual User Interfaces

Adobe Reader Multilingual User Interface (MUI) and Adobe Acrobat MUI simplify the process of installing different language versions. For organizations that operate across geographical boundaries, this feature can speed up deployment of any combination of supported languages. The MUIs enables you to roll out the same worldwide image of Reader or Acrobat with a single install job. Local users can then select the user interface language, or an administrator can set it through Group Policy for Organizational Units.

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 Reader XI and Acrobat XI, 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 the Acrobat XI 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.

Support for Microsoft System Center Updates Publisher (SCUP) catalogs enables you to automate updates to your Acrobat XI and Reader XI 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 XI and Reader XI 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 the Acrobat XI 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 Acrobat and 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.

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 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.

Content security

In today's computing environment, it is important not only to provide adequate security at the perimeter of your network (for example, a firewall) to keep unauthorized individuals from entering your network, but also to protect against your sensitive data, intellectual property, and other information assets from leaving your network, either unwittingly or knowingly.

To this end, Adobe supports an array of industry-standard mechanisms to help secure and authenticate the information stored in your PDF documents, including electronic signatures, rights management, and document best practices.

Electronic signatures

Electronic signatures save time and money compared to "wet," or original ink, signatures that reply on paper-based processes such as printing, faxing, or sending documents by overnight carrier. Electronic signatures help document authors and recipients ensure the integrity and authenticity of a document's contents. With Reader XI and Acrobat XI, you can easily sign documents using signature certificates that you create yourself or are issued by third-party certificate authorities that independently validate the identity of the participants.

Rights management

The Acrobat XI Family of products works with Adobe LiveCycle® Rights Management ES3 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. 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.

By combining the rights management capabilities in Adobe LiveCycle with the real-time data analysis and visualization solutions found in Adobe Insight, you can further reduce the risk of document leakage, determine who has accessed or printed protected files, and discover potentially malevolent end-user activities. Together, robust rights management capabilities and intuitive, end-user activity monitoring allow you to dynamically identify and track patterns of content access and use across your networks of systems and teams worldwide.

Consistent best practices

The improved Action Wizard feature in Acrobat XI 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 Acrobat XI Family of products, Adobe takes the security of PDF documents and your data to a whole new level. From extended application security to protect against the theft of your sensitive corporate data and intellectual property as well as block installation of dangerous malware on your computer systems and more granular JavaScript controls to integration with additional tools that make administering enterprise-wide deployments easier than ever before, Adobe Reader XI and Adobe Acrobat XI deliver greater levels of security at a lower TCO than any prior version of the Acrobat Family of products.

Plus, Acrobat XI and Reader XI are backed by the Adobe team of product security experts, the Adobe Secure Software Engineering Team (ASSET). Working together with the Adobe 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 Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

6/12