Delivering an information risk management strategy across the heterogeneous enterprise

Use Adobe® LiveCycle® Rights Management ES software to proactively protect sensitive information resident in the most widely used applications and files

Table of contents

1: Matching policies to the sensitivity level of data
2: Enforcing and controlling sensitive information assets
3: Manually securing sensitive documents
3: Adding protection to system-generated documents
4: Working securely with Microsoft PowerPoint presentations
5: Managing access to Microsoft Excel spreadsheets
5: Safeguarding content in Microsoft Word
6: Protecting sensitive information in PDF files
6: Securing collaboration among engineering teams
8: Summary

To succeed in today's global economy, businesses face intense pressure to produce and deliver better products and services to the market faster and more efficiently. To achieve this, they need to exchange sensitive information efficiently and extend their business processes to include partners and suppliers across industries and geographies with diverse regulatory environments. Organizations should proactively initiate an information risk management strategy to understand and prioritize risk in a consistent and repeatable way, and then target solutions that map risk profiles to protection levels. Information-centric solutions such as Adobe LiveCycle Rights Management ES enable this type of strategy by proactively protecting and controlling sensitive information at the source based on business policy, regardless of where the information resides or flows inside or outside the enterprise.

Ultimately, the lines-of-business and legal and compliance departments are not concerned with what documents or file types the sensitive information resides in, but they do require that the most sensitive information assets are discovered, protected, and ultimately audited to prove compliance. With this in mind, Adobe's Rights Management ES solution provides broad coverage for the most commonly used documents and file types for sensitive information in the enterprise, including Microsoft Office, PDF, and CAD files, enabling protection based on consistent policies set by the lines-of-business and legal and compliance departments, and executed by IT.

Matching policies to the sensitivity level of data

The term "policy management" is often overused, but meaningful in deploying a successful information risk management strategy. Information-centric policies have typically been the by-product of corporate or government bylaws that are rarely implemented in practice. However, with the advent of technologies like LiveCycle Rights Management ES, the lines-of-business can work in conjunction with legal, compliance, and IT to bring information-centric policy management to life in the enterprise.

Agreement on and development of these policies require that classification be married with enforcement and control to map appropriate protection to the risk profile of the information. With the Adobe LiveCycle Rights Management ES solution, information-centric enforcement and control policies can be created, managed, and dynamically updated at the document level regardless of the file type. These policies remain consistent regardless of whether the information resides in a Word document, PDF file, PowerPoint presentation, or any other commonly used file format. Effective policy management practices help organizations protect and dynamically control sensitive information without compromising the rate or volume of information exchange with internal and external constituents.

Enforcing and controlling sensitive information assets

Corporate confidential information

If confidential corporate information such as design and process drawings, patent information, trade secrets, or even source code is compromised, it can have an adverse effect on the business. So too can the loss of proprietary strategy and operations data such as customer lists, pricing information, patents, merger and aquisition discussions, or marketing strategy documents. This type of sensitive information typically resides in Microsoft Word and PowerPoint documents or in PDF files, so it is imperative to choose a solution that can provide protection across this spectrum of file types. Loss of control over these documents can have adverse effects, including loss of customer confidence, customer churn, and the erosion of competitive advantage from a product and market perspective. With the Rights Management ES solution, document access and usage rights can be based on the sensitivity level of the information and updated or revoked at any time, even if the document has been distributed outside the organization. As a result, organizations more confidently exchange sensitive information and collaborate more effectively in today's global business climate.

Regulated information

Regulatory compliance laws mandate that organizations keep confidential information under their control, protected from data breach. Failure to provide adequate protection against unauthorized access to regulated information, such as corporate financial data, human resources data, healthcare records, or personally identifiable information (PII), can have a variety of consequences. Penalties include fines, loss of customer confidence, and increased costs from legal and data breach notification fees. Sensitive information of this type is most often resident in Microsoft Excel and PDF files. Adobe LiveCycle Rights Management ES software reduces risk and liability in a regulated environment by enabling you to enforce control based on policies that map to the sensitivity level as dictated by the regulations. For those who have undergone classification projects or own data loss prevention (DLP) technology, the benefits derived from Adobe LiveCycle Rights Management ES can be even greater. Users can apply persistent and dynamic rights management policies directly to regulated information, regardless of where they have been transmitted or where they are stored.

Audit all actions taken on the information

As these information-centric policies are implemented, it is important to audit the who, what, and when of the organization's most sensitive information. LiveCycle Rights Management ES can offer fine-grained auditing capabilities at the document level to notify authors, business users, security administrators, and others of exactly what actions, such as editing, copying, and printing, have been taken on the document for audit and regulatory compliance purposes.

Use Adobe LiveCycle Rights Management ES to:

- Reduce the risk of theft of intellectual property and unauthorized disclosure of sensitive information and increase compliance effectiveness while exchanging documents with business partners
- Enhance the security of existing information systems by maintaining the capability to protect and control sensitive documents outside the system
- Discreetly extend and automate version control and manage document availability inside and outside the organization

Manually securing sensitive documents

The following steps detail how the Adobe LiveCycle Rights Management ES solution can help you rights-protect PDF, Word, Excel, PowerPoint, and CAD files.

1. Create the document that contains the sensitive information. The document can be created in one of the supported Microsoft Office or CAD applications, or it can be created in any other desktop application and then converted to an Adobe PDF file using Adobe Acrobat®, Acrobat Pro Extended, or Adobe LiveCycle PDF Generator 3D ES.
2. From within the native application, select a predefined security policy from a drop-down menu, or create a new one with customized access and usage rights. Apply the security policy to the document, and save the document.
3. Distribute the protected file by e-mail or on a CD, or post it to a website with the confidence that only designated people will have access to the file. No matter how the document is delivered or where the file is stored, the access and usage rights policy is automatically enforced.
4. When attempting to open a rights-protected file, the client contacts the rights management server to check for the current policy usage and access rights. Adobe LiveCycle Rights Management ES authenticates the recipient against credentials stored in the organization's authentication directory. Only after successful authentication can a recipient use the document, limited to the usage rights established in the current policy.
5. Adobe LiveCycle Rights Management ES captures an audit trail of all document activities, including the printing and opening of the protected document. The audit trail enables management to monitor how the information is used and to demonstrate that the information has been used only as prescribed by the policy.

Adding protection to system-generated documents

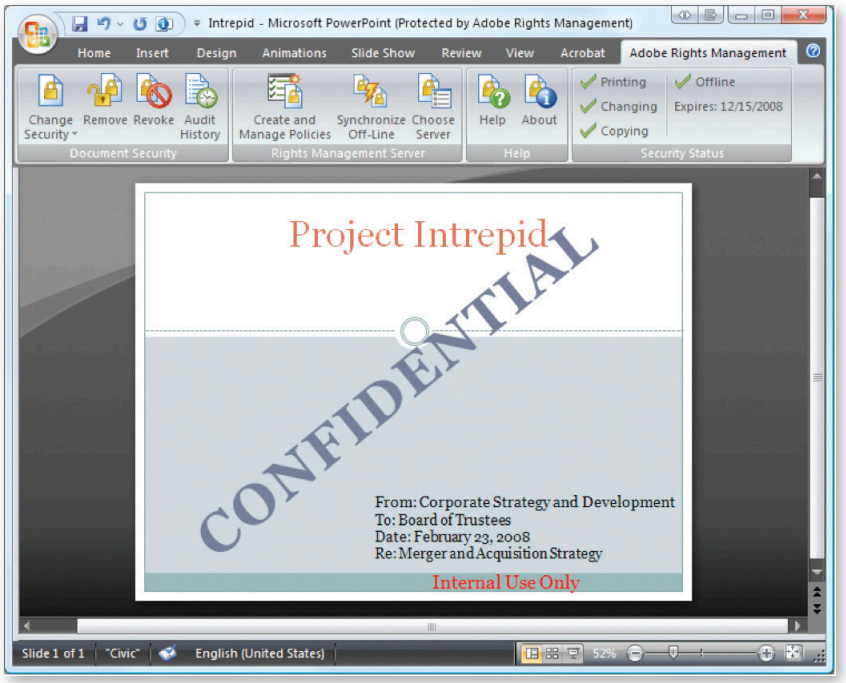
The following steps detail how the Adobe LiveCycle Rights Management ES solution can help you rights-protect documents generated as part of an automated process using multiple Adobe LiveCycle ES (Enterprise Suite) solution components.

1. Using Adobe LiveCycle PDF Generator ES, a document is created as an Adobe PDF file in response to a system-generated event. For example, a remote employee with VPN access rights requests an RFQ through an intranet page by clicking a link that triggers the system to generate and prepare the requested information for delivery. The document contains confidential customer information, requiring a security policy with specific access and usage rights that has been predefined for this use case.
2. Using LiveCycle Workbench ES, which is included with most LiveCycle ES solution components, LiveCycle PDF Generator ES automatically requests that Adobe LiveCycle Rights Management ES apply the appropriate policy to the document.
3. After the policy is applied, the employee receives the requested information as an attachment by e-mail or, in the case of large files, an e-mail that contains a link to download the file through an FTP server or web page.
4. Prior to opening the rights-protected file, the client contacts the policy server to authenticate the current access and usage rights policy. This helps prevent unauthorized users from accessing confidential information, even if the e-mail is accidentally forwarded or someone gains unauthorized access to the e-mail account. After Adobe LiveCycle Rights Management ES has authenticated the recipient, the individual can use the information in accordance with the usage rights established in the policy.
5. Adobe LiveCycle Rights Management ES generates an audit trail of the actions to help track how the information is used.

Working securely with Microsoft PowerPoint presentations

Collaborating with partners and customers electronically is risky—it requires maintaining the confidentiality of and control over sensitive information at all times, especially outside the enterprise. The Adobe LiveCycle Rights Management ES solution enables you to extend your business processes more securely outside your network. It protects business-critical and regulatory information against theft and misuse, and gives you greater assurance that only authorized individuals can access the protected information and use it as prescribed by preset usage rights. This protection enables you to engage with confidence in sensitive document-based processes and collaborate more securely and efficiently with extended teams and partners around the world.

It is critical for legal firms to have an easily accessible, secure, and engaging way to share documents with clients, co-counsel, and outside counsel. Using LiveCycle Rights Management ES, rights can be assigned to protect and control a PowerPoint presentation with sensitive information about a pending merger or acquisition.



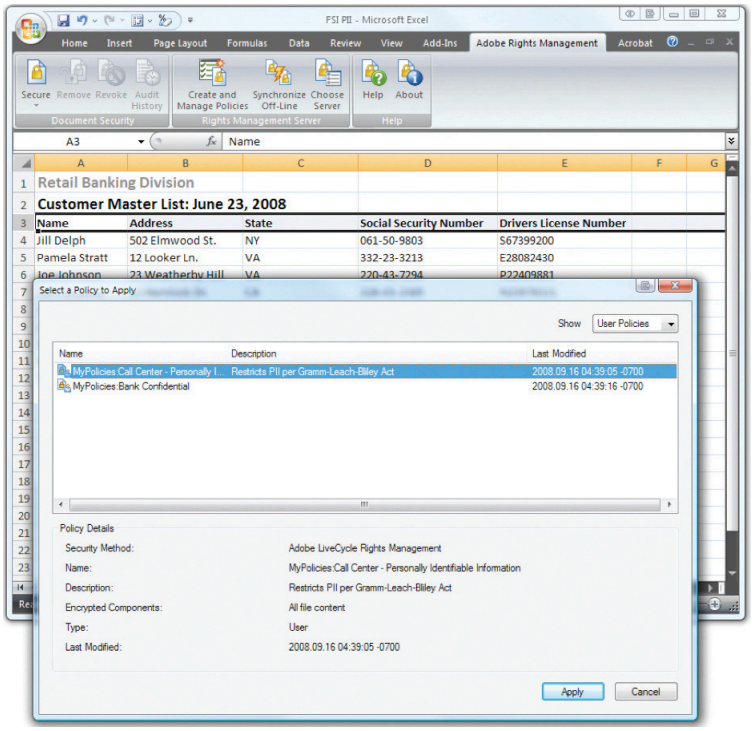
Viewing a PowerPoint presentation that is rights-protected using LiveCycle Rights Management ES. The Board of Trustees can view the presentation offline, while the corporate development team running the deal can change and print the document. Others involved in the deal, such as third-party litigators or due-diligence personnel, have restricted rights to print because they are potentially higher risk participants.

In another scenario, a senior sales engineer may draft a set of supporting PowerPoint slides describing technical aspects of the proposed customer solution in preparation for a major sales presentation. Because the contents of these slides are time-sensitive and strictly confidential, it is critical that the technical, sales, and marketing review processes be coordinated and controlled.

The author can set separate expiries and access permissions on the file for each group of reviewers, leveraging LiveCycle Rights Management ES integration with LDAP servers to automatically map rights characteristics for each group to corporate policy. Customized messages can be configured to assist users unable to access the file. For example, if a reviewer forwards the file to co-workers for comments, they can be directed to a help desk or to the author of the presentation to request access rights. Leveraging other LiveCycle ES solution components including LiveCycle Process Management ES, the PowerPoint presentation can be automatically routed through the review cycle, helping to ensure that deadlines are met.

Managing access to Microsoft Excel spreadsheets

It is important that financial institutions maintain regulatory compliance with laws such as the Gramm-Leach-Bliley Act, which typically mandate that sensitive PII is protected to limit the risk of identity theft. This information is typically kept in spreadsheet applications such as Microsoft Excel and can proliferate quickly into high-risk areas of the enterprise if not protected proactively. For example, information gathered at a call center and then stored locally on a laptop could be inadvertently e-mailed to the wrong person and ultimately become compromised.

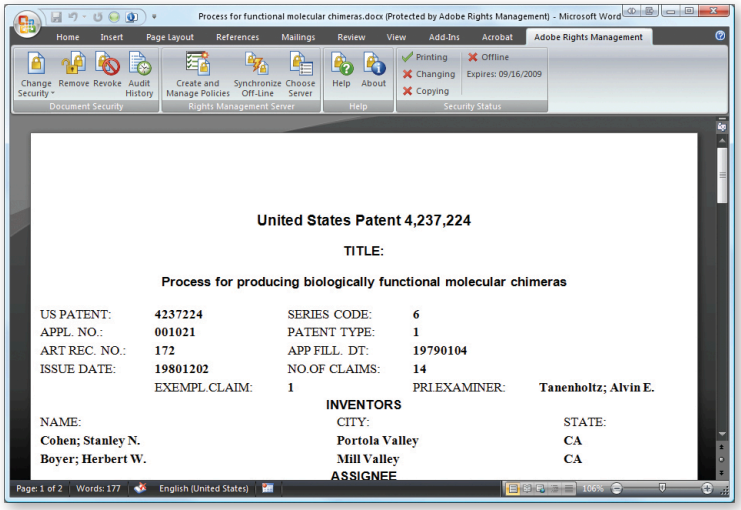


Policies can be applied to Excel files via MyPolicies to allow the author to initiate a pre-built enforcement policy. In this case, the policy pertains to enforcing sensitive PII to protect retail banking customers' identities.

For example, senior financial officers of a publicly traded mortgage company may share Excel spreadsheets extensively to consolidate, analyze, report on, and forecast financial results. Such documents expose the organization to significant risks of accidental or malicious disclosure of sensitive information to unauthorized individuals and of noncompliance liability in the event of an audit. By assigning rights management policies to the spreadsheet, they can prevent unauthorized access, distribution, and printing. Before distributing the spreadsheet, the creator can also choose to capture a record of every time it was opened, modified, printed, and closed for assessing use, mitigating risk, and demonstrating compliance. Leveraging the ability of Adobe LiveCycle Rights Management ES to integrate with popular archiving systems, the spreadsheet can be preserved in support of requirements for long-term preservation.

Safeguarding content in Microsoft Word

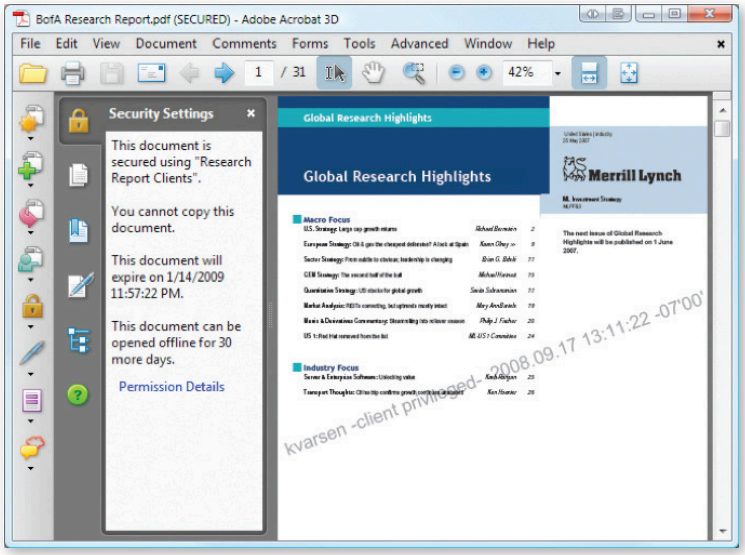
It is critical for legal firms to have an easily accessible, more secure, and engaging way to share legal documents with clients, co-counsel, and outside counsel. Using LiveCycle Rights Management ES, a lawyer can easily assign rights that protect a Word file from modification while saving the document. You do not need to use any additional software or have knowledge of the underlying LiveCycle infrastructure. Because the policy attributes are part of the document itself, it can be e-mailed or handed to outside counsel for review without needing to install special client software.



A U.S. patent in Microsoft Word that has been protected with LiveCycle Rights Management ES.

Protecting sensitive information in PDF files

As one would expect, LiveCycle Rights Management ES protects information in PDF documents, and enables users of Adobe Acrobat and Adobe Reader® to take advantage of rights management integration. PDF has become the de facto standard for printable documents on the web and is used in many business applications worldwide. With almost 700 million copies of Adobe Reader installed, protection can be applied to any document that can be opened in Adobe Reader. In many cases, hundreds of hours of time go into creating financial research reports, for example, yet the information leaks out into the market over the web and through e-mail, sharply decreasing its competitive value.



To help protect intellectual property, a policy is applied to a financial research report. The document is secured so that it is accessible only to authorized clients and cannot be opened by anyone else. It also has an expiration date, beyond which it is unusable, and specifies an offline usage policy in case someone wants to view the report remotely or on a plane where Internet access might not be available.

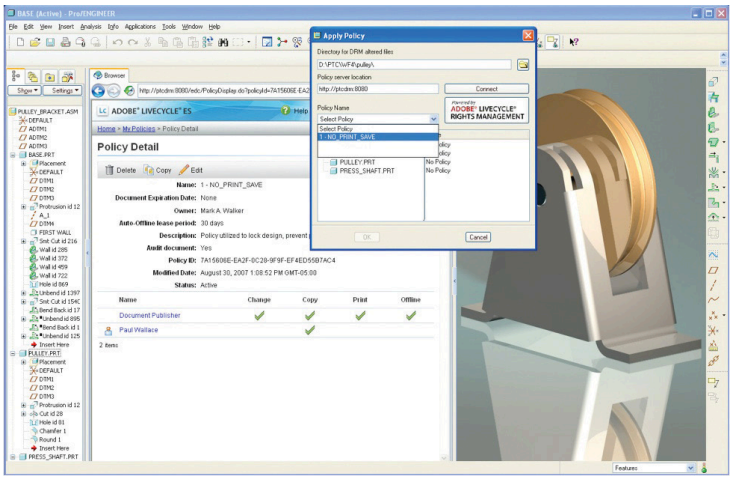
Securing collaboration among engineering teams

The manufacturing world has widespread requirements to protect sensitive intellectual property located in CAD documents. Manufacturers need to collaborate and exchange ideas throughout the product development process, which often requires that unprotected part designs be shared. Adobe LiveCycle Rights Management ES works with a number of CAD partners to help protect this information persistently, securing the supply chain and ensuring that a compromise of this information does not result in a loss of competitive advantage.

Pro/ENGINEER CAD files from PTC

LiveCycle Rights Management ES policies can be assigned to Pro/ENGINEER files, allowing fine-grained control of who can take specific actions. For example, a policy can be defined allowing only a specific person to take copy actions on a particular design. If an authorized user of the document tries to open an older version, the policy automatically revokes access to the older document and provides a URL to take the user to the latest copy. This revision control can maximize the efficiency of the supply chain process and drastically reduce the number of errors and time wasted on outdated designs.

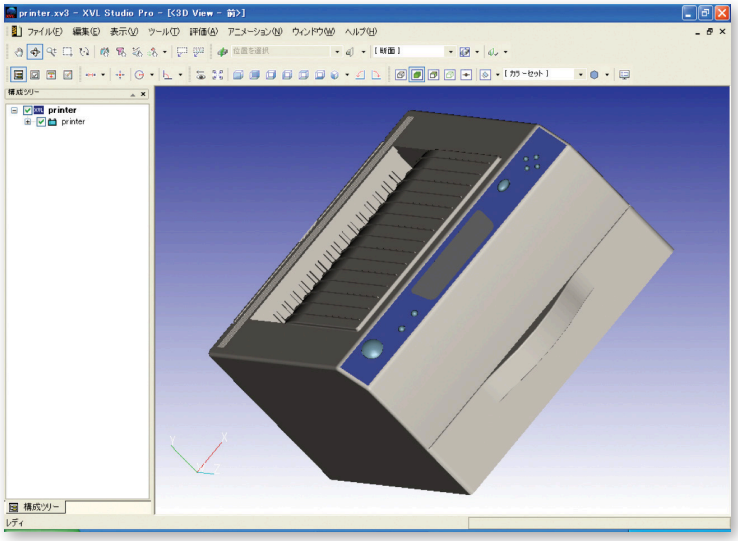
When the document is distributed to users, they can only take actions based on the policy rights that have been explicitly assigned to them. Attempts to complete operations for which users do not have permissions results in an error message.



Only Paul Wallace has the right to copy this design. He cannot change, print, or view the file offline.

Lattice Technology XVL files

Adobe provides rights enforcement of XVL files. For example, a vehicle manufacturer faced with ad hoc and inconsistent protection of intellectual property in XVL files risks sustaining extensive financial damage due to security leaks throughout its large external supply chain. By incorporating LiveCycle Rights Management ES with the company's existing ECM system and security infrastructure, it can achieve more effective collaboration with the assurance that valuable intellectual property is protected with complete audit trails of all XVL files.



LiveCycle Rights Management ES supports localized languages in Lattice Technology XVL files.

Summary

Sensitive information assets expose organizations to risks that can damage their reputation, compliance posture, or competitive position. Yet to succeed in today's global economy, businesses need to exchange sensitive information efficiently and extend their business processes to include partners or suppliers across industries and geographies with diverse regulatory environments. Information risk management strategies can be developed to help understand and prioritize risk in a consistent and repeatable way, and then target solutions that map risk profiles to protection levels. Information-centric solutions like Adobe LiveCycle Rights Management ES enable this type of strategy by proactively protecting and controlling sensitive information at the source based on business policy, regardless of where the information resides or flows, inside or outside the enterprise. The LiveCycle Rights Management ES solution provides broad coverage for all the most commonly used documents and file types for sensitive information in the enterprise, including Microsoft Office, PDF and CAD files, which can all be protected easily and consistently based on corporate policies.

For more information
www.adobe.com/livecycle

Adobe

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

Adobe, the Adobe logo, Acrobat, LiveCycle, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2013 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

91069492 1/13