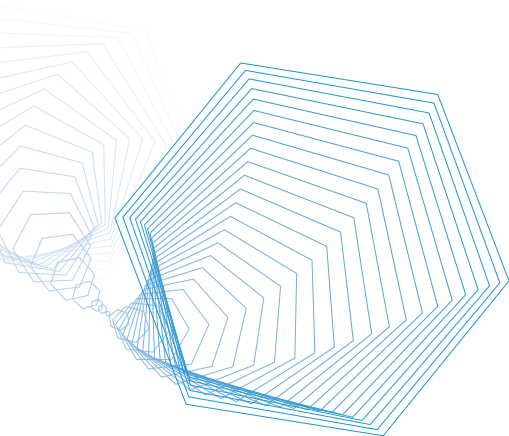


Adobe® LiveCycle™ Policy Server

Manage information access more securely
with dynamic, persistent document control

Critical business information must be protected at all times, even when it travels outside the organization. How do you continue to increase the ease and efficiency of your business operations with customers, partners and suppliers, yet ensure safe, secure information sharing?



ADOBE LIVECYCLE POLICY SERVER:

- Encrypts documents to control user access and rights
- Controls document access and use online, offline, and outside the firewall
- Applies expiration dates and validity periods to documents
- Revokes access to previously distributed documents
- Always knows when a document has been viewed, printed, copied, forwarded, and more
- Leverages group information and checks user credentials against existing authentication directories
- Extends version control, access control, and auditing beyond document and enterprise content management (ECM) solutions

Adobe LiveCycle Policy Server offers a convenient, effective solution for managing and monitoring the use of mission-critical electronic documents. Using Adobe LiveCycle Policy Server, you can consistently apply policies to control access and use of documents no matter where they are—online or offline, inside or outside your organization's network.

As an integral part of Adobe Document Services, a solution suite designed to automate and accelerate business processes, Adobe LiveCycle Policy Server helps you manage the complete document lifecycle more securely.

- Maintain control of electronic documents
- Dynamically manage document usage policies
- Extend the value of current IT investments in security and content management systems
- Reduce the cost of sharing information

Adobe LiveCycle software is built on a common server architecture based on Java 2 Platform, Enterprise Edition (J2EE) and XML, allowing for easy integration into enterprise infrastructures by providing Java application programming interfaces (APIs) and support for Web services protocols. Adobe LiveCycle is optimized for IBM® WebSphere® software and can be deployed on JBoss application servers.

Persistent document control

With Adobe LiveCycle Policy Server, you can encrypt documents and apply policies to more effectively control document access and use. Authors can assign permissions that specify a recipient's

level of access, such as restricting or allowing printing; copying, adding or removing pages; forwarding; or saving a document. Document use is easily monitored with a complete and detailed audit trail that keeps track of what each recipient did with a document, when, and how often. The document control is persistent because the policy is applied to the document at all times. No matter where a document is being used, you gain greater assurance that only the intended recipients have access.

Dynamic policy management

Adobe LiveCycle Policy Server makes it possible to manage document policies dynamically so that you can make policy changes without having to reissue documents after they are distributed. Simply change the policy on the server—such as revoking access to a previously distributed document, changing usage rights, or adding an expiration date—and Adobe LiveCycle Policy Server immediately updates the policies in all existing copies of the document.

Designed for enterprise integration

Built on industry-standard technologies, Adobe LiveCycle Policy Server enhances the value of your existing IT infrastructure. You can integrate Adobe LiveCycle Policy Server with current authentication and ECM solutions for cost-effective, centralized document control and administration. Adobe LiveCycle Policy Server accesses existing Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory implementations to authenticate recipients' credentials. And with ECM integration, you can extend document version control beyond these systems to ensure that the appropriate

SYSTEM REQUIREMENTS

Microsoft® Windows Server™ 2003, Enterprise Edition

- Intel® Pentium® 4 at 1GHz
- 1GB of RAM
- Two CPUs

Microsoft Windows® 2000 Server with Service Pack 2

- Intel Pentium 4 at 1GHz
- 1GB of RAM
- Two CPUs

Red Hat® Enterprise Linux® AS 2.1

- Intel Pentium 4 at 1GHz
 - 1GB of RAM
 - Two CPUs
- Sun™ Solaris™ 9
- Sun UltraSPARC III at 1.2GHz
 - 2GB of RAM
 - Two CPUs

Web Application Server/OS

- WebSphere 5.1 on Windows Server 2003, Enterprise Edition
- WebSphere 5.1 on Red Hat Enterprise Linux AS 2.1
- WebSphere 5.1 on Solaris 9
- JBoss 3.2.5 on Windows Server 2003
- JBoss 3.2.5 on Windows 2000 Server with Service Pack 2
- JBoss 3.2.5 on Red Hat Enterprise Linux AS 2.1

Database/OS

- Oracle9i on Solaris 9
- Oracle9i on Windows Server 2003, Enterprise Edition
- MySQL 4.x on Windows Server 2003
- MySQL 4.x on Windows 2000 Server with Service Pack 2
- MySQL 4.x on Red Hat Enterprise Linux AS 2.1

FOR MORE INFORMATION

For more information about the complete line of Adobe LiveCycle products, please visit www.adobe.com/security.

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

Adobe, the Adobe logo, Acrobat, Adobe LiveCycle, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. IBM and WebSphere are trademarks of International Business Machines Corporation in the United States and/or other countries. Linux is a registered trademark of Linus Torvalds. Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat is a trademark or registered trademark of Red Hat, Inc. in the United States and other countries. Solaris and Sun are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

© 2004 Adobe Systems Incorporated. All rights reserved. Printed in the USA.
95003814 8/04

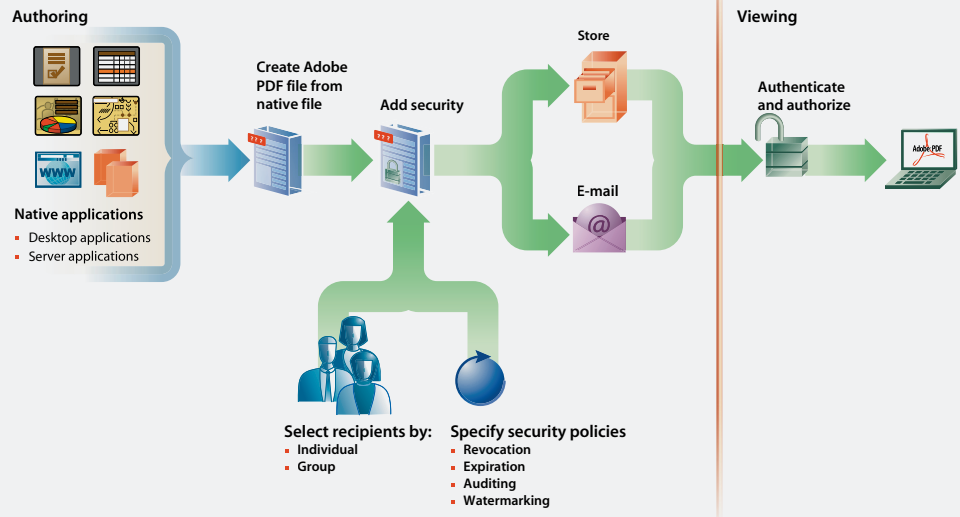


Figure 1: Managing Information with Document Control

This diagram offers a high-level overview for protecting electronic documents using Adobe LiveCycle Policy Server.

versions are in use after publication and distribution to people's desktops.

Easy document control online and offline

Authoring and viewing protected documents is easy and convenient thanks to tight integration with Adobe Acrobat® and Adobe Reader® software. Authors can apply security policies as they create Adobe PDF files from popular desktop applications including, Microsoft Office, Microsoft Outlook, Microsoft Internet Explorer, and AutoCAD. Recipients can view and work with secured documents online and offline using the ubiquitous, cross-platform Reader, which eliminates the need for additional software on their desktops.

Document control for author-generated documents

1. An author creates a document using a desktop application, such as Microsoft Word, and converts it to an Adobe PDF file using Acrobat.
2. Using Acrobat, the author can select an existing security policy from Adobe LiveCycle Policy Server or create a new one.
3. The policy is applied to the Adobe PDF file, and the author can distribute the file in a variety of ways, including by e-mail or on a CD, or post it to a Web site. No matter how the document is delivered, the policy goes with it.
4. Before allowing access to the document, Adobe LiveCycle Policy Server authenticates the recipient against

credentials stored in the organization's authentication directory.

5. The recipient can use the document only according to the controls established in the policy.
6. The author can check on the recipient's actions and change the security policy for the document, as well as any other documents he or she previously published.

Document control for system-generated documents

1. Using Adobe Document Services, a document, such as a customer's bank statement, is created as an Adobe PDF file in response to a system-generated event. Because the bank statement contains a customer's private information, a confidentiality policy is required.
3. Adobe Document Services automatically contact Adobe LiveCycle Policy Server for the appropriate policy. Once the policy is applied, the statement is delivered to the customer by e-mail.
4. Before allowing access to the statement, Adobe LiveCycle Policy Server authenticates the customer against credentials stored in the bank's customer authentication directory.
5. Adobe LiveCycle Policy Server will prevent unauthorized users from accessing the statement even if the e-mail is accidentally forwarded or someone gains unauthorized access to the e-mail account.

