

# Adobe® LiveCycle™ Policy Server

Manage information access more securely with dynamic, persistent document control

You need to protect your critical business information at all times. But how do you safeguard the privacy of sensitive documents distributed outside the organization?

#### USE ADOBE LIVECYCLE POLICY SERVER TO:

- Encrypt documents to control user access
- Control document access and use both online and offline, inside and outside the firewall
- Apply expiration dates to documents
- Revoke access to previously distributed documents
- Know when a document has been viewed, printed, copied, or forwarded—at all times
- Extend version control beyond document and content management systems

With Adobe LiveCycle Policy Server software, you can conveniently and effectively manage and monitor your business-critical electronic documents. Apply policies to control access to and use of documents at all times—online or offline, both inside and outside the enterprise network. An integral part of the Adobe Intelligent Document Platform, Adobe LiveCycle Policy Server helps you more securely manage all your document-based processes to:

- 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 with customers, suppliers, partners, and other constituents

#### Apply persistent document control

With Adobe LiveCycle Policy Server, you can encrypt documents and apply policies to increase control over documents. Allow document authors to easily 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. Easily monitor each recipient's use of a document, including when and how often the document is accessed. Document control is persistent because the policy travels with the document at all times. No matter where a document is being used, you gain greater assurance that only the intended recipients have access.

#### Manage policies dynamically

Adobe LiveCycle Policy Server makes it possible to manage document policies dynamically—so you can make policy changes without having to reissue documents after they are distributed. Simply change the policy—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 when they next communicate with Adobe LiveCycle Policy Server.

#### Integrate with and extend your existing enterprise infrastructure

Built on industry-standard technologies, Adobe LiveCycle Policy Server enhances the value of your existing IT infrastructure. Integrate the Adobe software with current authentication and enterprise content management (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 versions are in use after publication and distribution.

#### Protect documents both 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 ubiquitous, cross-platform, free Adobe Reader, virtually eliminating the need for additional software on their desktops.

Built on Java 2, Enterprise Edition (J2EE) and XML, Adobe LiveCycle products easily integrate with enterprise infrastructures through Java application programming interfaces (APIs) and support for Web services. Adobe LiveCycle software can be deployed on IBM® WebSphere and JBoss application servers.



## SYSTEM REQUIREMENTS

### Microsoft® Windows Server™ 2003

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

### Microsoft Windows® 2000 Server with Service Pack 2

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

### Red Hat® Enterprise Linux® AS 2.1

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

### Sun™ Solaris™ 9

- Sun UltraSPARC® III at 1.2GHz
- 2GB of RAM
- Two CPUs

### Web application server/operating system

- IBM WebSphere 5.1/5.1.1 on Windows Server 2003, Enterprise Edition
- IBM WebSphere 5.1/5.1.1 on Windows Server 2000 with Service Pack 2
- IBM WebSphere 5.1/5.1.1 on Red Hat Enterprise Linux AS 2.1 update 3 or later
- IBM WebSphere 5.1/5.1.1 on Sun 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 update 3 or later

### Database/operating system

- Oracle9i on Windows Server 2003
- Oracle9i on Windows Server 2000 with Service Pack 2
- Oracle9i on Red Hat Enterprise Linux AS 2.1 update 3 or later
- Oracle9i on Sun Solaris 9
- MySQL 4.0.18 and 4.0.20 on Windows Server 2003
- MySQL 4.0.18 and 4.0.20 on Windows 2000 Server with Service Pack 2
- MySQL 4.0.18 and 4.0.20 on Red Hat Enterprise Linux AS 2.1 update 3 or later

## FOR MORE INFORMATION

To learn more about Adobe LiveCycle Policy Server and the complete line of Adobe LiveCycle products, call 866-766-2256 or visit [www.adobe.com/products/server](http://www.adobe.com/products/server).

Adobe helps people create, manage, and deliver the highest quality digital content in the world. **Better by Adobe.™**

**Adobe Systems Incorporated**  
345 Park Avenue, San Jose, CA 95110-2704 USA  
[www.adobe.com](http://www.adobe.com)

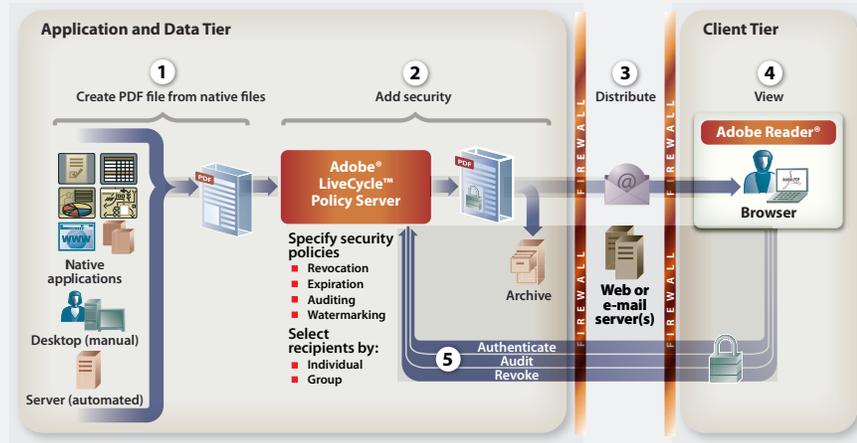
Adobe, the Adobe logo, Acrobat, Adobe LiveCycle, the Adobe PDF logo, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. IBM is a trademark 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.

95004536 1/04

## Managing information with document control

Adobe LiveCycle Policy Server enables enterprises to protect the confidentiality of sensitive documents inside and outside the firewall.



**Step 1.** Create PDF file manually from any member of the Acrobat family of products or automatically from Adobe Document Server, Adobe Central Pro Output Server, or Adobe LiveCycle Forms software.

**Step 2.** Apply security policy to the PDF file and assign security permissions to users.

**Step 3.** Store or distribute the PDF file via e-mail, the Web, or CD.

**Step 4.** User opens the PDF file after logging in to Adobe LiveCycle Policy Server.

**Step 5.** Adobe LiveCycle Policy Server audits user actions, including printing, opening, and form filling. Permissions are managed or revoked.

## How to control author-generated documents

The following step-by-step instructions illustrate how you can control author-generated documents using Adobe LiveCycle Policy Server.

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 selects an existing security policy from Adobe LiveCycle Policy Server—or creates a new one.
3. After applying the policy to the Adobe PDF file, the author distributes the file by e-mail or on a CD, or posts it to a Web site. No matter how the document is delivered, the policy is automatically linked.
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 is only permitted to use the document according to the controls established in the policy.
6. The author checks the recipient's actions and changes the security policy for the document, as well as for any other documents he or she has previously published.

## How to control system-generated documents

The following steps illustrate how you can control system-generated documents, such as customer bank statements, using Adobe LiveCycle Policy Server.

1. Using Adobe LiveCycle, a document is created as an Adobe PDF file in response to a system-generated event. The document contains confidential customer information, requiring a confidentiality policy.
2. Adobe LiveCycle automatically contacts Adobe LiveCycle Policy Server for the appropriate policy. Once the policy is applied, the document is delivered to the customer by e-mail.
3. Before allowing access to the document, Adobe LiveCycle Policy Server authenticates the customer against credentials stored in the company's customer authentication directory.
4. Adobe LiveCycle Policy Server helps prevent unauthorized users from accessing the document even if the e-mail is accidentally forwarded or someone gains unauthorized access to the e-mail account.

