EMC²
where information lives®

EMC Documentum IRM Client for PDF

Control access to PDFs anytime, anywhere

Organizations are under increasing pressure to share their intellectual property and valuable information electronically with colleagues, partners, and customers. Typically, organizations implement multiple layers of security such as firewalls, file encryption, and authentication to secure information. However, these security approaches can't protect documents once they're distributed beyond corporate boundaries.

Patented rights management

With EMC® Documentum® software, your organization can now address this security loophole. Documentum native capabilities go well beyond authentication, access control, auditing, and SSL encryption and include repository encryption, mandatory access control, electronic signatures, and digital shredding. With EMC Documentum Information Rights Management (IRM) Services complementing the native security of the Documentum platform, your organization can protect sensitive content no matter where it exists—within or beyond the firewall.

Information Rights Management Services is a flexible application that enables secure document sharing and provides total control over your electronic information—even after it is in the hands of recipients. Leveraging patented rights management technology, IRM Services continuously protects documents during and after delivery.

Documentum IRM solutions are suitable for a wide range of industries, including manufacturing, financial services, healthcare, and government services. Typical applications include executive communications, secure outsourcing, policy enforcement, and regulatory compliance.

The Documentum IRM Services family encompasses modules for securing documents, e-mails, and mobile mail:

- EMC Documentum IRM Client for PDF
- EMC Documentum IRM Client for Microsoft Office
- EMC Documentum IRM Client for E-Mail

Dynamic control of distributed PDFs

With Documentum IRM Client for PDF, you control who can access a PDF document. You can prohibit printing of a PDF or a select portion of it, disable copy/paste, prevent screen capture, and watermark pages if printing privileges are granted. IRM Client for PDF lets you expire access to PDFs at any time and provides a complete audit trail reflecting all document activity.

Unlike traditional security products that only protect content during delivery, a PDF protected by Documentum IRM Services is always encrypted and usage permissions are enforced—no matter where the document is located. Organizations or individual document authors can change the permissions on distributed information at any time. For example, if access to a document needs to be revoked, the access permissions for that document can be modified and enforced on all copies of the document, wherever they are located.

The Big Picture

- Control access to PDFs
- Enforce permissions—no matter where a PDF is located
- Prohibit printing of a PDF or a select portion of it
- Expire PDFs at any time
- Obtain a complete audit trail that details document activity, such as viewing or printing

Feature	Benefit
Control over expiration	Allows organizations to automatically expire information in accordance with corporate security policies. Also allows old revisions of documents to be expired to ensure that recipients are accessing only the most current versions.
Dynamic revocability	Allows organizations to automatically revoke access to documents if an employee departs or a business relationship terminates.
Dynamic watermarking	Organizations can dynamically insert a custom watermark into a document that includes the viewer's name, the date, and header information such as a Document ID or time, to deter authorized viewers from printing and distributing the document.
Detailed audit trail	Organizations can continuously track document activity including what pages were viewed, by whom, when, from where, for how long, and whether they were printed.
Windows single sign-on authentication support	Allows users to protect and view documents without requiring additional authentication steps.
Work off-line mode	Lets recipients access protected documents when they are not connected to the Documentum IRM Server. In this mode, the document policy originally established by the author is still enforced.
Integration with existing security infrastructure	Organizations can leverage existing authentication systems and LDAP user directories for creating document policies, thereby reducing administrator involvement.

EMC²
where information lives®

Take the next step
To learn more about EMC Documentum solutions for information rights management, visit **www.EMC.com** or call **800.607.9546** (outside the U.S.: +1.925.600.5802).