EMC Documentum IRM Client for Microsoft Office

Protect Microsoft Office files within and beyond the enterprise

Today 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, you can now address what has become a security loophole for organizations. 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 Services complementing the native security of the Documentum platform, you can protect sensitive content no matter where it exists—within or beyond the firewall.

Documentum Information Rights Management Services is a flexible, secure document-sharing application that gives you total control over your electronic information—even after recipients have it. 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, health care, 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 Adobe Acrobat
- EMC Documentum IRM Client for Microsoft Office
- EMC Documentum IRM Client for E-Mail
- EMC Documentum IRM Client for RIM BlackBerry

The Big Picture

- Control access to business documents and prevent them from being forwarded to unauthorized recipients

- Enforce permissions—no matter where the document is located

- Prohibit printing of a business document or a select portion of it

- Expire documents at any time

- Obtain a complete audit trail that details document activity, such as viewing or printing

- Leverage tight integration with Microsoft Office applications to preserve your users' existing workflow and minimize training requirements

Applications for Documentum IRM Client for Microsoft Office

- Executive teams can securely share confidential presentations and revoke access to all electronic copies at any time

- HR teams can securely collaborate on restructure plans and compensation spreadsheets

- Marketing and product development teams can securely share and collaborate on product design specifications and price books with outsourcing partners

- Corporate legal counsel can ensure their organization's compliance with customer non-disclosure agreements

Tight integration with existing applications and workflow

EMC Documentum IRM Client for Microsoft Office provides tight integration with Microsoft Office applications to preserve your users' existing workflow and minimize training requirements. Content owners can enforce information security policies and track access to information right from their desktop applications. Organizations can also automate protection and policy enforcement by integrating IRM Services within third-party content management systems, e-mail gateways, and portal applications.

Features	Benefits
Seamless integration with Microsoft Office applications	Simplifies user experience and minimizes training requirements
Persistent protection	Ensures that information is protected at rest, in transit, and even while it's being viewed by recipients
Dynamic policy control	Allows content owners to change user permissions (view, forward, copy, print, or edit) and recall documents after they're distributed
Secure editing	Allows users to collaborate on and modify documents without worrying that they will be accessed by unauthorized recipients
Automatic expiration	Access to information can be revoked at any time; allows version control and information security policies to be enforced wherever content is distributed
Policy-based watermarking	Centrally applies a printed or visual watermark on documents to communicate data classification and to deter unauthorized forwarding and copying by recipients
Continuous audit trail	Provides confirmation that information was delivered and viewed and offers proof of compliance with your organization's information security policies
Leverages existing authentication security infrastructure	Reduces administrator involvement and speeds deployment by leveraging user and group information that exists in directories and authentication systems
Tight integration with existing workflow	Allows information security policies to be applied by content owners at the desktop or automatically applied by integrating IRM Services with third-party content management systems, e-mail gateways, and portal applications

EMC²
where information lives®

Take the next step

To learn more about EMC Documentum solutions for information rights management, visit http://software.emc.com or call **800.607.9546** (outside the U.S.: **+1.925.600.5802**).