

EMC Documentum ApplicationXtender with Information Rights Management

Maintain control and protect sensitive business-ready content

The Big Picture

- Maintain control over sensitive business-ready content residing outside the repository and even beyond the firewall
- Enable secure sharing of sensitive documents with internal and external users
- Protect Microsoft® Office documents, PDFs, and any file that can be exported as a PDF
- Dynamically revoke rights or alter documents, no matter where the content physically resides

All organizations have sensitive or confidential information stored in repositories, file folders, documents, or even as e-mail file attachments. While there are many solutions to securely store the information, a primary concern is how to protect the information after it leaves the repository. There is always a risk that someone will share this sensitive information with an unauthorized third party, but there is also a risk of someone inappropriately sharing information by copying documents onto their external storage devices or e-mailing documents as file attachments.

EMC® Documentum® ApplicationXtender® with Information Rights Management (IRM) ensures that confidential information remains secure, even after it leaves the repository. Rights are enforced by a document policy that defines who, what, when, or whether a document can be copied, printed, or taken offline, and controls other settings, such as watermarking, rights expiration, and whether guest access is allowed. The policy is attached to the document and the content is encrypted prior to exporting it to the end user. Protection is persistent no matter where the content resides or where it travels.

ApplicationXtender with IRM provides a tight integration between Information Rights Management and the ApplicationXtender document management system. Importantly, ApplicationXtender only places IRM policies on a document after the document is exported from the ApplicationXtender repository. This key capability enables the content owner to maintain control of the document—internally and even outside the firewall.

Persistent protection at all times

Organizations continually deploy and enhance firewalls and anti-spyware software, install VPN networks, and implement other secure methods to successfully protect their information. But at times, such security measures fall short. Today, the majority of costly security breaches and anomalies are not the result of intruders from the outside accessing confidential internal information, but rather the result of insiders taking or sending confidential material beyond an organization's perimeter walls.

ApplicationXtender with IRM can assign a rights protection policy to a document anytime the document is exported from ApplicationXtender or sent as an e-mail file attachment. For example, IRM policy enforcement can safeguard hospital patient records, even if the laptop they reside on is lost or stolen. Such security breaches could cost the hospital millions of dollars. But, if the hospital uses IRM, those patient records can be protected—even after the laptop is stolen. Once the data loss is detected, the hospital can set an immediate expiration on the records by changing the IRM policy in real time, minimizing risk exposure and embarrassment.

Dynamic controls in place

ApplicationXtender with IRM provides persistent controls for content owners by enabling them to dynamically revoke or alter permissions after the content has been delivered. Once an employee leaves the organization, access to all confidential content can be revoked. Even if that person copied confidential content or information from the repository to a memory stick, CD-ROM, or USB flash drive prior to leaving the company, the files would not be accessible and remain secure, existing only as unusable and unrecognizable encrypted files.

More secure viewing, editing, copying, and printing controls

ApplicationXtender with IRM provides more secure controls, whether a user is viewing the content or providing permissions to edit, copy, or print the content. All forms of electronic copying are controlled—selecting text and copying and pasting it, using a screen capture mechanism such as the Print Screen button on the keyboard or any of the numerous screen-scrape software tools available. Printing can be prevented altogether, or can be allowed with certain stipulations, such as printing with dynamic watermarks that place a user's name or ID on all printed copies.

For an organization that sells bids, proposals, and service contracts to other organizations, information is treated as highly confidential. With IRM, the organization can ensure that documents are not forwarded to unauthorized users, especially competitors. IRM policies also control what recipients can do with documents, such as print, copy, or edit, with policies that go wherever the company's information travels. Policies are supported offline as well. IRM enables organizations to:

- Enforce and preserve the value of confidential property
- Prevent unauthorized sharing or copying of bids, proposals, and service contracts
- Watermark authorized usernames and time stamps on every page of the protected document

Additional content management controls

Integrating rights management with content management extends the functionality of ApplicationXtender document management. As an example, versioning can be enforced, ensuring that only the current version is accessible to users, even when copies are stored on local desktops. When older versions expire, users are directed back to the repository to retrieve current versions. IRM protections can also be automatically applied to document renditions, ensuring that content is available, but still protected in all forms.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

Take the next step

To learn more about ApplicationXtender with Information Rights Management, visit www.EMC.com or call 800.607.9546 (outside the U.S.: +1.925.600.5802).