Safe collaboration using information-centric security

With the document security feature in Adobe Experience Manager forms, you can proactively protect sensitive documents, and control and track their usage—from creation to archiving.

Table of contents

In today's global, digitally networked economy, organizations are under pressure to quickly and efficiently deliver better products and services to the market. Organizations are constantly exchanging or selectively distributing documents that contain sensitive information—internally with employees, externally with partners, and through digital self-service to consumers. At the same time, maintaining control of information has never been more difficult. Wireless networks, the proliferation of mobile devices, cloud services, and the popularity of bring your own device (BYOD) make it difficult to protect document information even within the enterprise network—let alone outside of it.

The best way to protect personal, company confidential, or classified content is to embed security within the document. This information-centric approach does not rely on network or application security alone to secure data. A recent study* shows that 72% of IT and IT security respondents agreed that document security is a valuable component in a layered defense to protect the confidentiality, integrity, and authenticity of information.

Adobe Experience Manager forms transforms complex forms and document transactions into simple engaging digital experiences—anytime, anywhere, on any device. The document security feature in Adobe Experience Manager forms proactively protects and controls sensitive information from theft or misuse, regardless of where the information resides or travels—inside or outside the enterprise. Government agencies and enterprises in many industries are using the document security feature in Adobe Experience Manager forms to:

- Secure intellectual property
- Maintain public safety by protecting classified documents
- Protect personally identifiable information (PII)
- Support compliance objectives
- Meet data governance and protection mandates

Document security allows any organization with sensitive information to:

- Match policies to the sensitivity level of data
- Protect common document files
- Streamline document protection and consumption
- Store protected documents
- Track all actions taken on protected information
- Strengthen document protection with real-time visual analysis

* Ponemon Institute. 2014. *Global insights on document security.*

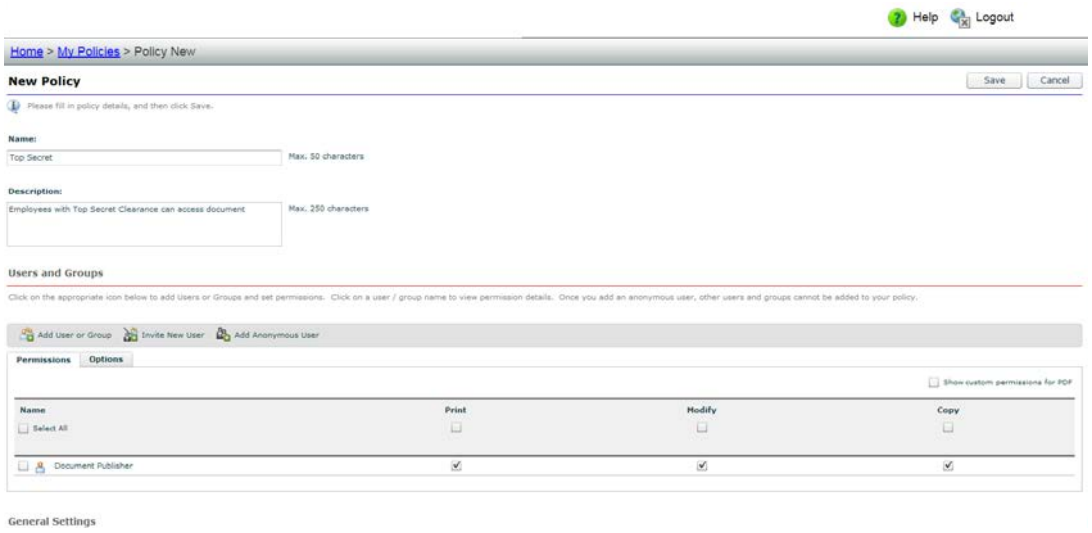
Match policies to the sensitivity level of data

Policy management is part of a successful information risk management strategy. Information-centric policies have typically been the by-product of corporate or government bylaws that were sometimes not implemented in practice.

With document security, lines of business can work in conjunction with legal, compliance, and IT to make information-centric policy management a reality for digital documents. You can match different classes of documents, depending on their risk profile, with the appropriate policy. You can create, manage, and dynamically update information-centric enforcement and control policies at the document level. Document security policies define:

- Which users or groups of users can access the document
- What users or groups are allowed to do with protected documents (for example, print, copy text, make changes, or add signatures or comments)
- Whether or not to audit document events
- How long a document remains valid and accurate (for example, for what duration, or to a certain date)
- Whether users or groups can use protected documents when they are not connected to the Internet, and for how long
- Whether dynamic watermarks are applied
- Whether to have an external authorization provider or policy decision point (PDP)

These policies remain with the document regardless of where it travels. You can change policies at any time, or even revoke usage rights, even after documents have been distributed. Document security protects intellectual property, classified documents, and PII from theft or misuse.



The document security feature in Adobe Experience Manager forms allows business users to create granular document usage policies that match corporate information policies.

Control intellectual property

Intellectual property—from product or process designs to patents—is often contained in documents. So too is proprietary data such as customer lists, merger and acquisition discussions, or marketing strategy documents. In the wrong hands, this information can impact a company's brand, damage its reputation, and quickly erode its competitive advantage. With the document security contained in Adobe Experience Manager forms, you can:

- Confidently exchange sensitive information and collaborate more effectively in today's global business climate
- Tailor document access and usage rights to the sensitivity of the information, track its use, and revoke usage rights at any time—even if the document has been distributed outside the organization

Control secret information

With hacktivism and targeted attacks on the rise, governments around the world are increasingly concerned about security breaches. Whether leaks are accidental or intentional, the release of classified documents can have grave consequences and threaten national security. The document security in Adobe Experience Manager forms protects documents with strong FIPS 140 Suite B AES 256-bit encryption—making it the document security solution of choice for many public safety organizations.

Control regulated information

Regulatory compliance laws mandate that organizations protect confidential information from data breach. Failure to provide adequate protection against unauthorized access—including financial data, human resources data, personal health information, or PII—can have a variety of consequences. Penalties include fines, loss of customer confidence, and increased costs from legal and data breach notification fees. The document security feature in Adobe Experience Manager forms reduces risk and liability in a regulated environment by allowing you to enforce policies that map to the sensitivity level mandated by the regulations. For organizations that have completed classification projects or have data loss prevention (DLP) technology, document security offers additional benefits. Users can apply persistent and dynamic policies directly to regulated information—regardless of where they transmit or store the documents.

Protect common document files

Sharing documents electronically is a common way to efficiently extend information to teams, partners, and clients down the hall or around the globe. Many common document formats can contain sensitive information. Document security seamlessly protects PDF and Microsoft Office files. The document security software development kit (SDK) also allows organizations to extend document protection to other types of files, such as design or production drawings. You can use your regular business applications while securely sharing necessary information with team members, partners, or clients.

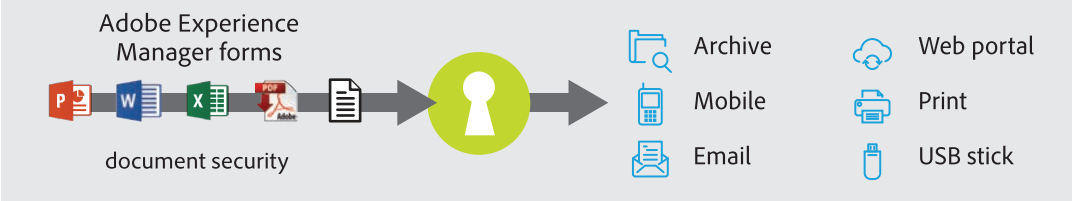
Streamline document protection

Maintaining the confidentiality of and control over sensitive information should not impact the efficiency of your organization. Sharing information is critical to the success of many business initiatives, and nontechnical users should not have to learn new software or perform complicated processes to protect sensitive information.

Document security in Adobe Experience Manager forms allows users of Microsoft Office and Adobe Acrobat to natively protect information contained in documents. Business users can assign usage policies to documents while saving the document from within the native application. Users simply select a predefined organizational security policy from a menu, or create a new one with customized access and usage rights. Then, they apply the security policy to the document and save the document.

The document security feature uses LDAP or Microsoft Active Directory servers to automatically map rights characteristics for each group to corporate policy. A custom service provider interface allows organizations to authenticate against other user domains. Document security works with strong user authentication systems, including single sign-on (SSO), security assertion markup language (SAML), and public key infrastructure (PKI). It also integrates with certificate-based authentication systems, such as the Common Access Card (CAC) and the Personal Identity Verification (PIV) used by the U.S. government, or the eID card used by Belgian citizens.

In addition to manually securing sensitive documents, other features in Adobe Experience Manager forms automatically protect bulk or system-generated documents, such as PDF statements or documents leaving a document management system. The document security feature can use the authorization and policy controls applied by the document management system to protect documents.



From within popular document applications, document security applies persistent security policies—protecting them as they travel through all channels, online or offline.

Simplify document consumption

It's easy for authorized users to access protected documents. Authorized recipients can use free, ubiquitous Adobe Reader or the Adobe Reader mobile app to access protected documents. Microsoft Office users need only the free document security extension for Microsoft Office, which automatically contacts the document security server when recipients attempt to access a protected Office document. Depending on how the security policy is defined, authorized users may need other credentials to access the document, such as username and password, or a smart card.

To assist document recipients, authors can configure customized messages to help users unable to access the file. For example, if a reviewer forwards the file to co-workers for comments, they can be directed to a help desk or to the author of the file to request access rights. Or, if a document has been revised, the author can alert recipients when they open an older version, and include a hyperlink to the up-to-date version.

Store protected documents

Document security integrates with Adobe Experience Manager sites, assets, and other enterprise content management (ECM) systems, allowing business users to easily find, store in a central repository, and selectively share protected documents with authorized users through intranet sites or web portals.

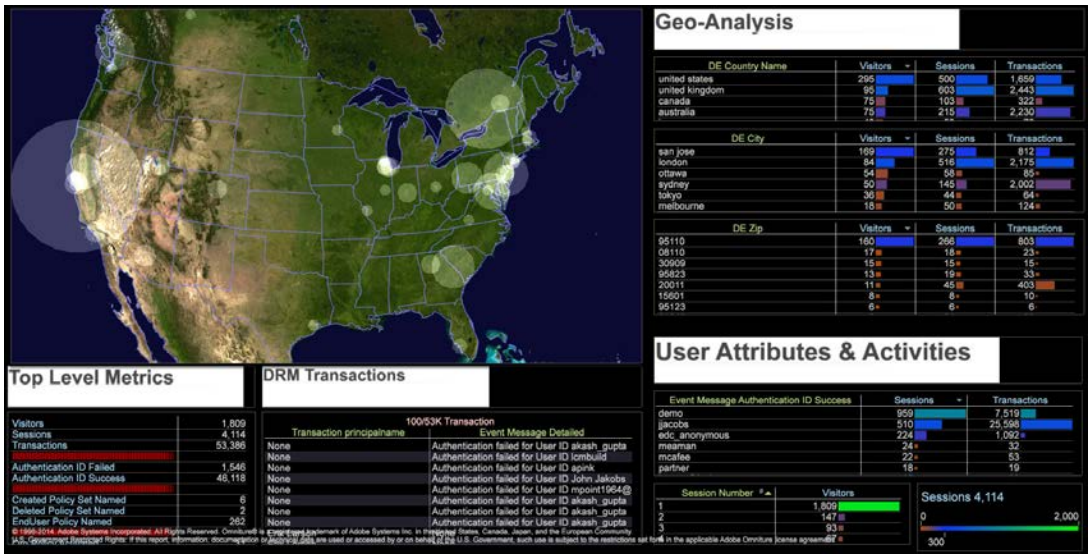
As an Adobe Managed Service, the document security in Adobe Experience Manager forms is a cloud-ready solution that can be securely deployed using Amazon Web Services in a private, single-tenant architecture.

Track all actions taken on protected information

As you implement information-centric policies, it is important to track who is accessing your organization's most sensitive information. The document security feature records who accessed a document and all of the actions he or she performed—for example, viewing, editing, copying, or printing. Actions by authors, such as creating a new version of a document, and administrative actions performed on policies are also audited. The audit trail allows management to monitor how sensitive information is used and to demonstrate that the information has been used only as prescribed by the policy. This data helps meet internal audit requirements and regulatory compliance objectives.

Strengthen document protection with real-time visual analysis

While tracking the effectiveness of document protection is critical, being able to quickly act on that information can further improve your compliance posture or business performance. Organizations can leverage Adobe Analytics data workbench (formerly Adobe Insight) capability to collect, process, and quickly analyze large volumes of constantly changing document security data captured by Adobe Experience Manager forms. Powerful visualizations give a comprehensive view of all protected documents in real time. Data segmented by user, document policy type, actions performed on documents, geographies, and more, gives you a complete understanding of how sensitive information is being used. This data can form actionable insights easily shared with key stakeholders. For example, users employing a certain authentication method may consume fewer protected documents, leading to further investigation. Or you can create alerts to proactively notify administrators of suspect activity, such as users printing a large amount of documents.



The data workbench capability of Adobe Analytics tracks protected documents in real time.

Summary

Compromising sensitive information can damage an organization's reputation, compliance posture, or competitive position. Yet to succeed in today's global economy, government agencies and businesses need to exchange sensitive digital information efficiently with clients, business partners, or their own employees—24x7. Developing information risk management strategies allows organizations to understand and prioritize risk in a consistent and repeatable way, and then target solutions that map risk profiles to protection levels. Document security should be a key pillar of any organization's information risk management strategy.

Document security contained in Adobe Experience Manager forms proactively protects and controls sensitive information contained in PDF and Microsoft Office documents based on business policy—regardless of where the information resides or flows—for its entire lifecycle. Detailed audit trails and integration with the data workbench capability in Adobe Analytics allows organizations to visually track document usage around the globe and take decisive actions based on real-time data.

For more information

www.adobe.com/go/aemforms

Adobe

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

8/15