

ITAR and EAR Compliance with EMC Documentum

Protect your confidential information within and outside the firewall

The Big Picture

- Provides ITAR and EAR compliant security for confidential information wherever it resides—in the repository, downloaded to a laptop, or in transit (for example, sent via e-mail)
- Helps companies and government agencies actively control, secure, and track sensitive information wherever it resides
- Ensures that only authorized recipients can view, copy, print, or edit information
- Allows content owners to revoke access after external distribution

The ITAR and EAR security regulations

The International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) were established by the U.S. government to control the export of defense-related technology and services listed on the U.S. Munitions List. Under these regulations, products and services become classified as “ITAR Controlled” and then require very strict security and access control.

Specifically, all information and material related to ITAR Controlled technology may only be shared with “U.S. Persons” unless a license or special exemption is obtained from the U.S. Department of State. And heavy fines are imposed for not only tangible transfers of technology and information but also situations in which an export has been “deemed” to occur, such as sales presentations and proposals to non-U.S. persons or non-U.S. entities or the accessing of controlled information by authorized personnel when traveling outside the U.S. The range of information controlled under these regulations is broad and includes not only the products themselves, but also designs, test data, processes, software, and others.

To address ITAR and EAR today, most organizations employ traditional firewall security, employ strict hiring practices, and maintain completely separate and redundant data centers in order to control access to ITAR-related information. But these types of solutions don’t scale. They also present fundamental organizational challenges and a competitive disadvantage as the industry moves to a global supply chain.

EMC solution

EMC offers an alternative to these challenges—EMC® Documentum®. Documentum secures all content types, providing a protected vault for all of your organization’s unstructured information—whether or not it’s ITAR controlled. Security features include advanced identity management for dynamic access control, enabling you to systemically prevent access to ITAR-controlled information from non-U.S. persons and from U.S. persons when located outside of the U.S. In addition, EMC Documentum Information Rights Management secures ITAR-controlled information outside the repository, for example when it’s been downloaded to an employee’s laptop or sent as an e-mail attachment. These combined capabilities enable enterprises to comply with both ITAR and the EAR “deemed export” rules in a systematic, controlled manner.

Securing your information

Documentum delivers the unique ability to dynamically control and manage who gets to view, edit, copy, or print e-mails and documents—and who does not. Information is encrypted and persistently protected at rest, in transit, and even while it’s being viewed by recipients. This gives your organization the freedom to collaborate with colleagues and business partners anywhere while ensuring that sensitive information doesn’t end up where it shouldn’t.

Leveraging patented rights management technology, Documentum gives you complete and dynamic control over ITAR and EAR-controlled information, including the ability to:

- Determine who can access a document both online and offline
- Prevent unauthorized recipients from viewing documents
- Prohibit printing of an entire document
- Disable copy/paste and screen capture capabilities
- Watermark pages if printing privileges are granted
- Expire or revoke document access at any time
- Track all document activity through a complete audit trail

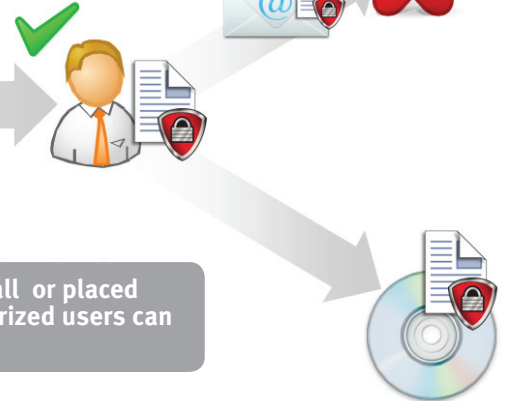
Achieve ITAR and EAR compliance with:

- [EMC Documentum Content Server](#)
- [EMC Documentum Trusted Content Services](#)
- [EMC Documentum Information Rights Management](#)

Key security features

- **Authentication, authorization, and auditing:** Documentum provides a flexible authentication framework that supports not only the ID/password challenge but also enables plug-ins for advanced authentication—such as biometrics, RSA Secure ID tokens, or X.509 certificates. Documentum authentication can be validated in real time against LDAP directories. Documentum provides highly granular access control (authorization) at the object level with a multitude of access levels. Finally, every event is tracked by a secure audit trail.
- **Repository encryption:** Documentum prevents intruders from accessing information by encrypting content within the repository. This capability protects content against an operating system-level security breach and enables you to securely store backup media containing information assets in encrypted form.
- **Encrypted communications:** With Documentum, content is encrypted both inside and outside the repository. Documentum transmits content securely between servers and clients. Employing strong data traffic encryption based on SSL, Documentum prevents “eavesdropping” security breaches and gives system architects more flexibility in designing systems with components that function both within and outside the firewall.
- **Dynamic and logic-based access controls:** Documentum can enforce security and individual access control policies based on combinations of rules and requirements. For example, content owners can define and change user permissions (view, copy, print, watermarks, take offline, view activity) and recall or expire content even after distribution. Documentum policies work for logic statements such as “need to know” or “ITAR controlled,” combining individual access clearances with project-specific security measures. This feature can be used for mandatory access control (MAC), giving the organization the ability to control the privileges on content, rather than allowing users to set discretionary privileges. Additionally, access controls can be dynamic, depending on changing factors such as a user’s role or geographic location. And Documentum provides the ability to automatically map ACL-based permissions into information rights management policies that control the content outside the Documentum repository.
- **Automatic expiration:** Documentum provides the ability to automatically revoke access to documents, e-mails, and attachments at any point, thus allowing information security policies to be enforced wherever content is distributed or stored.
- **Digital shredding:** Documentum provides a secure way to dispose of information through digital shredding. This technology ensures that information cannot be retrieved even by employing forensic methods that analyze residual magnetism on the storage media.

Content is persistently protected, regardless of where it goes.



Even when sent beyond the firewall or placed on removable storage, only authorized users can access content.

EMC Documentum protects information inside and outside of the firewall

Proven track record

EMC Documentum information rights management (IRM) helps global companies and government agencies to properly control ITAR and EAR-regulated content, and actively control, secure, and track sensitive information wherever it resides—within a workgroup, across departments and agencies, or with partners and suppliers outside the firewall. The seamless integration of Documentum platform security and Documentum IRM Services makes Documentum the most secure content infrastructure on the market.

EMC and partner content management solutions

This solution is one of many content management solutions offered by EMC and its partners.

EMC and its partners deliver content management solutions that help organizations to solve business problems specific to their function or industry. Built on the EMC Documentum platform, and combining EMC and partner technologies and services, these solutions help organizations streamline and automate processes, increase productivity of teams and individuals, address their information compliance and retention requirements, foster creative work, and lower the cost of operations.

EMC and partner content management solutions are designed to shorten deployment cycles as well. These solutions encompass a full range of integrated EMC products and professional services, combined with EMC-certified partner technologies and professional services. The combined industry experience and process expertise of EMC and our partners help you achieve maximum value in minimum time.

About EMC

EMC Corporation (NYSE: EMC) is the world's leading developer and provider of information infrastructure technology and solutions that enable organizations of all sizes to transform the way they compete and create value from their information. Information about EMC's products and services can be found at www.EMC.com.

EMC²
where information lives[®]

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 ITAR and EAR compliance with EMC Documentum, visit www.EMC.com or call 800.607.9546 (outside the U.S.: +1.925.600.5802).