EMC² where information lives®

EMC Documentum Security and Trusted Content Services

Protect your valuable information assets

The Big Picture

- Provides a secure repository for all types of unstructured information
- Ensures content security inside and outside the repository
- Offers built-in platform security plus powerful add-on security features through Trusted Content Services
- Seamlessly integrates with existing enterprise security and identity management infrastructure
- Achieves Common Criteria certification required by the US Department of Defense and other security-sensitive customers around the world

EMC® Documentum® secure, enterprise content management solutions ensure your organization's information remains secure—across business processes, as it is handled by users inside and outside the firewall, and from creation through archiving. Now you can implement and enforce organization-wide policies and controls that cannot be overridden by unauthorized individuals. The EMC Documentum repository secures all content types, providing a protected vault for all your organization's unstructured information.

Key security features

The EMC Documentum security platform comprises an unmatched set of comprehensive, flexible, and easy-to-use services, preventing unauthorized access to the proprietary information your employees and customers rely on.

- **Authentication, authorization, and auditing:** The Documentum core platform provides a flexible authentication framework that supports not only the ID/password challenge but also enables plug-ins for advanced authentication—such as biometrics, tokens, or X.509 certificates. Documentum authentication can be validated in real time against LDAP directories. The Documentum platform 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.
- **Identity management:** The Documentum platform integrates with industry-leading LDAP directories so it can participate in the enterprise-wide identity management infrastructure. Because the platform synchronizes users and user groups with LDAP directory servers, you do not need to independently manage Documentum identities. The platform also supports federated identity environments and multiple directories.
- **Single sign-on (SSO):** Your Documentum-based solutions can participate in single sign-on infrastructure across organizations by supporting industry-leading SSO frameworks such as RSA Access Manager.
- **Encrypted communications:** The Documentum platform transmits content securely between servers and clients. Employing strong data traffic encryption based on SSL, the Documentum platform prevents "eavesdropping" security breaches and gives system architects more flexibility in designing systems with components that function both within and outside the firewall.

- **Digital rights management (DRM):** The Documentum platform controls and protects documents even after they are retrieved from the repository and shared. With Documentum Information Rights Management Services, the system maintains complete control over access privileges outside the Documentum repository.

In addition to the core security features in the Documentum platform, EMC Documentum Trusted Content Services (TCS) adds a specialized layer of security measures and access control features.

- **Dynamic and logic-based access controls:** Documentum TCS can enforce security and individual access control policies based on combinations of rules and requirements. Use logic statements to establish access control provisions such as "need to know" or "top secret," 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.
- **Repository encryption:** Documentum TCS prevents intruders from accessing information even if they obtain unauthorized access to repository files at the file-system or storage level. This capability protects content against an operating system–level security breach and enables you to securely store back-up media containing information assets in encrypted form.
- **Electronic signatures:** Documentum TCS enables you to associate electronic signatures, which are stored as objects in the Documentum repository, with any information object or event such as process tasks. The signatures support FDA-compliant signature manifestation and contain a hash-checksum that verifies the authenticity of signed content. Electronic signatures are the basis for digital signatures, which enable signing with a higher level of authentication provided by the application.
- **Digital shredding:** Documentum TCS 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.

Proven track record

The Documentum enterprise content management platform is the secure content vault used by the most demanding and security-aware customers in the world—financial institutions, utilities, manufacturing companies, life sciences organizations, and government agencies.

Take the Next Step

To learn more about Documentum security and Trusted Content Services, visit us online at **http://software.EMC.com** or call **1.800.607.9546** (outside the U.S.: +1.925.600.5802).

EMC² where information lives®

EMC Corporation
Hopkinton
Massachusetts
01748-9103

1-508-435-1000
In North America 1-866-464-7381

Data Sheet
S12750507V2