

EMC Documentum Security

A Comprehensive Overview

Abstract

This white paper explains how the reliance on electronic information increases the need for security and why it is especially important to ensure a secure enterprise content management infrastructure. It details the core security features of EMC Documentum Content Server, the central component of the Documentum enterprise content management platform, and the enhanced security available through Documentum Trusted Content Services.

4/12/2007

Copyright © 2007 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com

EMC², EMC, Documentum, NetWorker, RSA, and where information lives are registered trademarks and Centera is a trademark of EMC Corporation. All other trademarks used herein are the property of their respective owners.

S11960407V3

Table of Contents

Raising the stakes: Security and electronic information	4
The importance of security to enterprise content management	4
The EMC Documentum content management platform—secure at the core.....	4
Platform security—Documentum Content Server.....	5
Added security with EMC Documentum Trusted Content Services	12
Information rights management	14
Common Criteria Certification.....	16
EMC Documentum—Delivering security you can trust.....	17

Raising the stakes: Security and electronic information

Information security has always been a concern of business and government. Trade secrets, military plans, profit and loss figures, and legal filings are just a few examples of the intellectual property these organizations feel compelled to protect from intruders and from many of their own employees.

Security concerns aren't limited to digital information. If a hard copy proprietary document leaves a company hidden under an employee's raincoat, it's just as devastating as if it were snatched electronically. But the increasing reliance by business and government on electronic information raises the security stakes exponentially. Digital content is so fluid and portable. With a thumb-sized flash drive, anyone with access could easily pilfer hundreds of important documents. And if an ambitious hacker with malicious intent breaches a corporate or government network, the potential damage is practically incalculable.

For governments, geo-political uncertainties also increase the possible risks associated with less than robust security. And for business, compliance demands and regulatory scrutiny have a security dimension as well. Financial institutions, for example, cannot meet their regulatory obligations regarding the safety of customer information without highly developed security procedures and technologies.

The importance of security to enterprise content management

Enterprise content management enables an organization to use a consolidated content infrastructure to create, manage, deliver, and archive all of its electronic content. It permits all content applications to leverage content management repositories and makes repository content accessible to employees throughout an enterprise no matter how geographically dispersed it may be. The benefits of enterprise content management are many: improved business processes, greater worker productivity, streamlined collaboration, and increased content accuracy to name just a few.

Enterprise content management systems typically become the system of record for an organization's most valuable information. Consequently, it is of paramount importance that the content management infrastructure be secure—from outside intrusion as well as internal trespassing. Without adequate security, one of an enterprise content management system's key strengths—its ability to centralize and simplify access to content—poses a significant threat to information assets. Content silos, on the other hand, make information harder to access for everyone, including those to whom access should be denied.

The EMC Documentum content management platform—secure at the core

Many of the world's most security conscious organizations deploy the EMC® Documentum® enterprise content management platform to manage and protect their information assets. At federal, state, and local governments in the United States and abroad, and at industry leaders in pharmaceuticals, finance, energy, and aerospace and defense, Documentum has earned the trust that only comes when information security is given the highest priority.

Security is not a feature that has been added as an afterthought to the Documentum platform. It is as much a part of the Documentum architecture as the ability to manage and control billions of content objects. For ultra sensitive projects requiring the highest levels of secrecy and access control, platform security enhancements are available through Documentum Trusted Content Services.

Platform security—Documentum Content Server

Most platform security features are built directly into the central component of Documentum—Documentum Content Server.

Authentication

To access content stored in the Documentum repository, users must authenticate—prove to the system that they are who they say they are. Default authentication validates a username and password, but Documentum does not store passwords. It leverages the existing operating system passwords instead. Functionality such as required password syntax or password aging is controlled by the OS. Augmenting OS functionality, the Documentum platform:

- **Enables login thresholds to prevent “brute force attacks”**
A brute force attack is a code-breaking technique that employs processing power to quickly go through all the permutations and combinations of numbers and characters that could comprise a password. Login thresholds limit the number of attempts to a small set (typically three). When that number is exceeded, the user account is locked to prevent further attempts.
- **Enforces session timeouts**
Administrators can set a time after which the system terminates any inactive session. This prevents illegitimate access to the workstation of a user who was “stuck at the water cooler.” This capability is usually combined with a screensaver that locks access to an end-user’s workstation.
- **Validates users within Documentum or against a directory server in real time**
Credentials presented as a response to an authentication challenge can be validated internally by Documentum Content Server or externally against a directory server in real time. This capability enables Documentum to participate within a corporate identity management infrastructure.
- **Audits logins in the Content Server log**
Just like any event in Documentum, all authentication attempts—whether successful or not—are tracked in a central audit log. This audit trail enables subsequent analysis of any authentication issue.

The authentication framework

Documentum Content Server authentication is based on an open architecture that can employ additional means of authentication beyond the default username and password pairs. This open framework permits plug-ins for external authentication authority, web single sign-on (SSO), and multifactor authentication and supports a variety of advanced security options such as biometrics, and X509.3 certificates—public key infrastructure (PKI), token cards, and smart cards.

Web single sign-on (SSO)

SSO is a desirable feature for many organizations because it delivers improved security, boosts user productivity and frees CPU cycles from authentication requests. It eliminates the need for users to remember multiple user names and passwords or to write them down where they can easily be stolen. SSO also reduces the volume of help desk calls requesting password resets.

Web SSO delivers several key business benefits:

- **Improves end user experience**
Web single sign-on protecting multiple web applications improves user experience by eliminating

re-authentication requirements. Fewer passwords or authentication challenges enables easier security policy compliance.

- **Manages risk**
Centralized, policy driven authorization consolidates application access and reduces the risk inherent in distributed, and often separately managed, access control lists embedded within applications.
- **Ensures compliance**
Centrally managed access enables organizations to rapidly demonstrate who should have access and who *actually* accessed protected resources.
- **Reduces costs**
Centralized access control reduces the administrative workload of managing disparate access control lists. Single-sign on also drives down help desk costs through minimized password reset calls.

Documentum Content Server leverages its authentication framework to participate in a web SSO infrastructure. Web SSO with RSA® Access Manager is supported out of the box through configurable options. RSA Access Manager enables the use of stronger authentication methods including RSA SecurID, digital certificates, and custom authentication methods.

Customers can also choose to integrate with CA Netegrity SiteMinder by using additional plug-ins, standard development tools, documented APIs, and sample plug-in source code for Netegrity SiteMinder available in the Documentum Content Server Administrator's Guide.

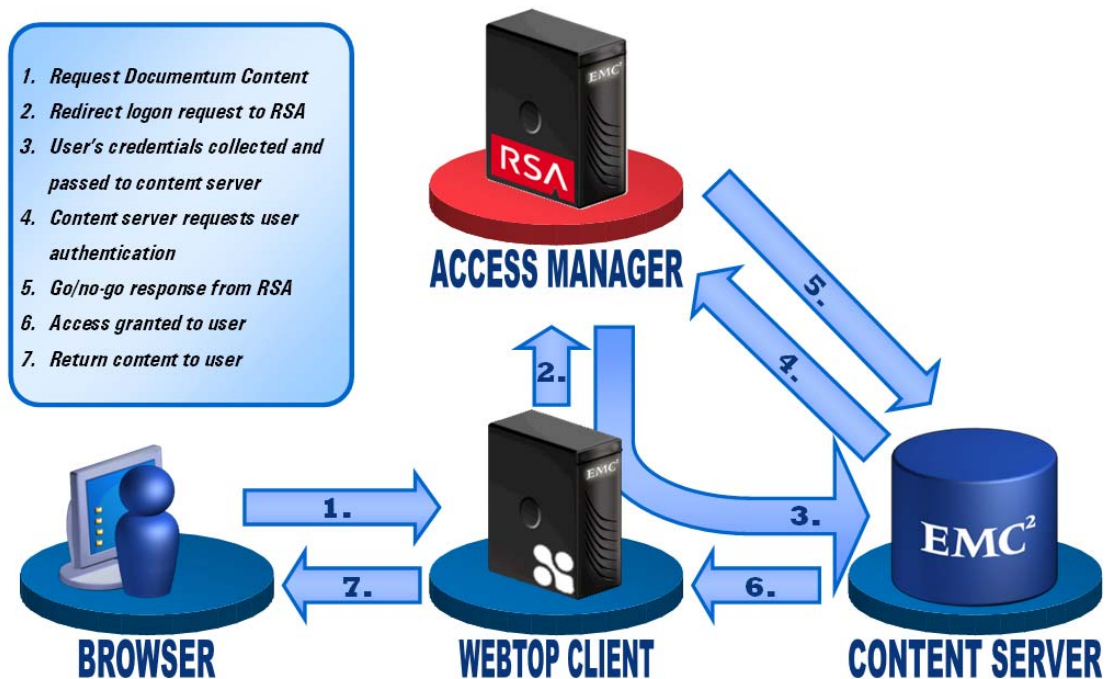


Figure 1. Authentication process using RSA single sign-on authority.

The authentication framework mixes authentication methods with RSA Access Manager, which delivers authorization. Supported authentication types for RSA Access Manager are user name/password, RSA SecurID, X.509 certificates, and custom methods.

External authentication support for EMC Documentum Web Development Kit

EMC Documentum Web Development Kit (WDK) contains a service that can delegate authentication to one of several providers, such as a manual repository, J2EE principal, or an SSO plug-in. Those wishing to use SSO from RSA or CA with Documentum clients based on Documentum Web Development Kit, should use the built-in SSO plug-in to enable their SSO manager. This delegation service bypasses the standard WDK authentication challenge component and can support SSO protection across more than one Documentum application. Single sign-on behavior can be achieved using a J2EE principal with another application (e.g. a portal application using an identity server) or using pass-through authentication (also sometimes known as silent sign-on) with an operating system or other framework.

Identity management

The Documentum platform is designed to integrate seamlessly within the corporate IT infrastructure, including enterprise identity management. Documentum Content Server supports connection to multiple directory servers and features integrations with common enterprise directories such as:

- Microsoft Active Directory
- Sun ONE Directory Server
- Oracle Internet Directory

Directory access services are delivered through industry-standard Lightweight Directory Access Protocol (LDAP). Integration enables enterprise-wide synchronization of users and user groups. Documentum administrators do not have to create users and groups individually within Documentum Content Server, which can be a daunting task when thousands of users are involved. Simplification and centralization of membership management increases the security of all participating systems. Decentralized management may create vulnerabilities due to inconsistencies between systems and a greater probability of administrator error.

The synchronization of users and user groups with a directory occurs at regular intervals set by the administrator. Instant synchronization can also be initiated by the administrator in case of an emergency. Directories use a federated model for administration, a model supported by Documentum. Federated administration provides a central point of control for a geographically distributed Documentum system. As a result, administrative costs can be significantly lowered.

Benefits and features of the Documentum identity management integration include:

- Use of industry-standard LDAP
- Encryption of the LDAP communication using SSL
- Real-time authentication against enterprise directories
- Reduced administration costs
- Greater security through simplification and centralization of user management

Authorization

Authorization (also referred to as access control or entitlement) determines what content can be seen by whom. Documentum assigns authorization at the object level through access control lists (ACLs), which are automatically applied to objects as they are created. By applying authorization at the object level, every

content object, version, and rendition, and every container for content assets from folders to repositories is governed by an ACL throughout its lifecycle.

Robust authorization capabilities ensure that only the appropriate users have access when that access is required. It also reduces the complexity of the enterprise content management system and simplifies navigation by removing from view content that users are not authorized to access.

Documentum lifecycle management can be used to automatically modify access control settings for an object as it is promoted and demoted throughout its lifecycle. For example, promoting a content object from “In review” to “Approved” could change the access control from RELATE, for a small group of reviewers, to READ for all users.

Access privileges

An ACL can grant access privileges to a particular content asset based on:

- Explicit assignment to an individual user
- Membership in a user group
- The role that a user has been assigned

Documentum provides seven levels of basic permissions (access privileges):

- **None**—Objects in the repository cannot be seen. This reduces complexity by hiding content that is irrelevant to the user. It is also an effective way to hide a sensitive document or project.
- **Browse**—Objects can be seen but not read.
- **Read**—Objects can be opened and read but not changed.
- **Relate**—Users can create a relationship between a given object and other objects. This level of access is typically used for annotations that are stored as separate objects with a relationship to the annotated content.
- **Version**—Users can make changes to a content asset but cannot overwrite an existing version. Changes are saved in a new version.
- **Write**—Users can make changes to a content asset and save them without creating a new version. This degree of access is usually restricted to the content owner.
- **Delete**—Users have the right to delete content assets.

Standard permissions are cumulative—each level automatically grants all access rights from the levels below it. A user with a WRITE permission to a particular object, for instance, can also browse, read, relate, and version the object, but cannot delete the object.

In addition to basic DELETE permission, Documentum provides DELETE_OBJECT permission, which grants deletion privileges while denying other levels of access. Using this “flattened” delete permission, a user can delete an object without the right to read, relate, version, or write it. This capability enables the corporate archivist, librarian, or records manager to expunge content according to retention policy without being exposed to its subject matter.

Documentum also provides five levels of extended permissions:

- **Change location**—Users can change the location of a content asset from one folder to another. By default, users with BROWSE permission or greater for an object are automatically granted CHANGE LOCATION permission.
- **Change permission**—Users can change an asset’s standard permissions without being the content owner.
- **Change owner**—Users can change the owner of a content asset without being the owner. This is important when a project is being reassigned and the original owner is unavailable.
- **Execute procedure**—Users can execute an external procedure, such as creating a rendition, on an object. All users with BROWSE permission automatically inherit EXECUTE PROCEDURE permission.
- **Change state**—Users can change a content asset’s lifecycle state.

Dynamic groups

A user group can be declared dynamic, enabling applications to move users in and out of groups at run time. The movement of users in and out of a group can be done only by authorized applications, not end users. A dynamic group is a variation of role-based security and is implemented as an additional property of group objects.

Combined with the multi-dimensional access control (MAC) described below, dynamic groups can be used to differentiate access privileges based on various external factors. For example, an application equipped with a global positioning system (GPS) to fix a user’s location could use the dynamic group assignment rule to grant user access based on continent, country, or home office location. Users might have WRITE access from one location and only READ from another.

Application access control

This level of security requires a client application to present a valid token when connecting to a repository. It ensures that only authorized applications can have access to the repository and protects content from unauthorized access.

Access control and governance with EMC Documentum rooms

Collaboration requires additional ways to deal with security that enable ad-hoc processes and support a self-administration model. With EMC Documentum Collaboration Services, a Documentum repository can contain rooms, which are secured areas within the repository that restrict access to a defined membership. Rooms provide users a secure virtual ‘place’ to do work where only those who belong to a room can see its content. Adding or removing users is as easy as adding or deleting them from the room’s member list.

Rooms can be set up manually by users for various projects or triggered automatically by business processes and events such as an insurance fraud investigation. In this case, a room is generated for field managers to collect sensitive case data, including pictures, videos, reports, and testimonials. Members discuss, review case materials, add notes, and participate in workflow processes to resolve the case. Upon resolution, the room or portions of it can remain in the repository, where its content can be indexed, audited, secured, filed as records, and archived.

Rooms have expanded the Documentum access control model to enable the following capabilities:

- **Access restrictions**—Access to a room is restricted to members of the room. Other users cannot access a room object regardless of its locations or ACL.
- **Member list and local roles**—Room owners can create local groups and roles without the intervention of an administrator. Members can view a list of all users, groups, and roles that are room members. Local groups and roles only have access to objects governed by that room.

- **Governance**—A governed object is one whose ACL is ruled by a room, and for which access is limited to the room member list. The membership of a room is defined by all the users in the members group. This group is used when setting the “required group” entry in a governed object’s ACL (see multi-dimensional access control).
- **Self administration**—Room owners manage room membership and permissions, including creation and deletion of local groups.
- **Home page**—In the client, viewing a room object reveals its home page. Home pages have tabs to manage membership and a banner graphic on each page to identify the room.
- **Identification**—Users can turn on a governing indicator in the column preferences to distinguish objects that belong to a room wherever they are located in a repository.

When a room is created, it automatically generates four groups: members, owners, contributors, and visitors. The groups assign users different roles for the room. They are implemented as groups, although they are used as roles.

Owners act as room coordinators while contributors are participants. Every room user belongs to one of these groups, both of which are private to the room. That means that any access privilege is restricted to the room and does not apply to the rest of the repository. These two groups are automatically assigned to every object (through the ACL) that is governed by the room, providing uniform default permissions.

The members group is composed of owners and contributors. Every user is required to be in the members group before being granted access to any governed object. This provision keeps the room isolated from a security point of view, although it physically resides in the same repository as other rooms and content objects. Collaboration Services does not require a license of Trusted Content Services to enable multi-dimensional access control (MAC). MAC is included in the Collaboration Services license. This security mechanism permits a repository to be open to external users such as contractors or suppliers who remain restricted to a particular room without compromising the entire repository.

The visitors group is used to track room visitors and is reserved for future use.

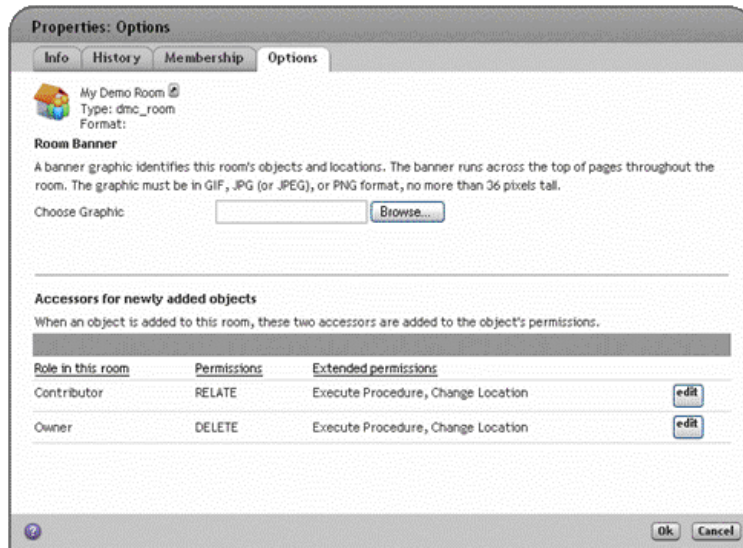


Figure 2. A Collaboration Services room home page includes easy access to tabs for setting up properties, inviting members, and other administrative tasks.

Auditing

Very simply, an audit identifies who participated in an event, what was done, and when. Enterprise content management audit capabilities deliver three significant benefits:

- Compliance—Audits are mandated in many regulated environments
- Security—Audits identify and trace security breaches
- Efficiency—Audits track system trends and can be used to improve business planning

Every event that occurs within the Documentum content management platform is audited, and all audits are stored in the Documentum repository as audit objects. Auditing is fully configurable using Documentum Administrator.

Audit objects can be accessed for analysis and reporting through Documentum Query Language (DQL) or through an ADO.NET interface provided by Documentum ADO.NET Services. The ADO.NET interface enables the creation of applications to leverage audit trails for reporting or the use of off-the-shelf reporting tools. Audit objects are stored in the repository with a secure signature using the SHA-1 hashing algorithm and 168-bit encryption.

Encrypted communication

Using the secure sockets layer (SSL) standard, all data traffic can be encrypted between Documentum Content Server and Documentum clients, including Documentum Desktop and any WDK-based client such as Documentum Webtop. Additionally, data traffic between Documentum Content Server and directory servers can be encrypted using SSL. Documentum Content Server can be set up to use secured or unsecured ports and clients can be mandated to connect through secured ports only. Documentum SSL employs the ADH (Anonymous Diffie-Hellman) algorithm with 1024-bit key size for key exchange. Data encryption uses the AES algorithm with 256-bit keys.

Encrypted communication prevents eavesdropping, ensures data privacy, increases the flexibility of network architecture, and allows directory servers or Documentum Content Server to be placed inside or outside a DMZ.

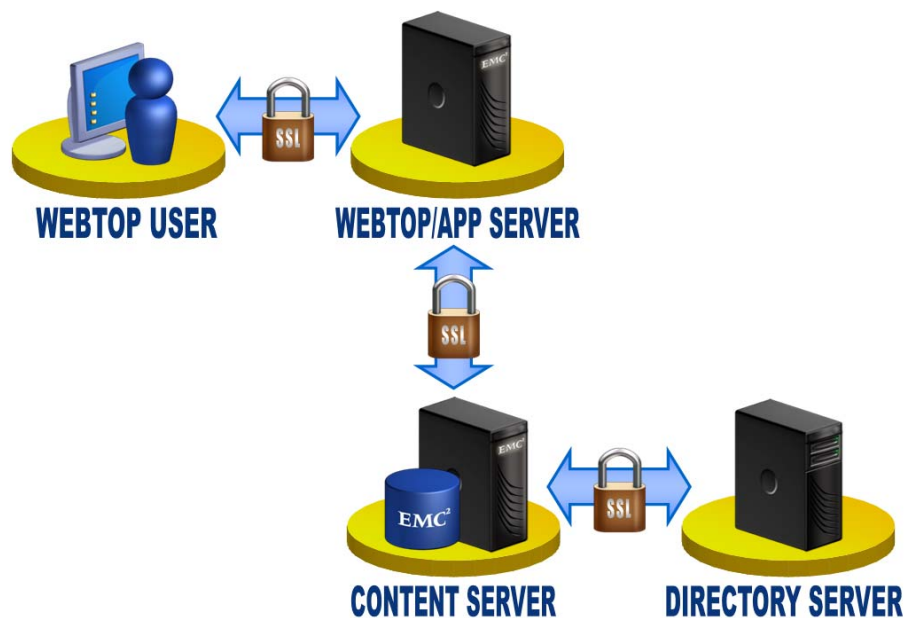


Figure 3: Data privacy provided by communication encrypted using SSL.

Added security with EMC Documentum Trusted Content Services

EMC Documentum Trusted Content Services (TCS) is an optional product that provides an extra layer of security and complements the core security features of Documentum Content Server. TCS is deeply embedded within the server. Its capabilities can be enabled with a valid license key.

TCS permits even the most security conscious organizations to create unmatched protection for their information assets. The features provided by TCS include:

- Repository encryption
- Electronic signatures
- Multi-dimensional access control (MAC)
- Digital shredding

Repository encryption

TCS enables encryption of the file stores that host content assets in the Documentum repository. The encrypted file store prevents access to content files on the operating system level. For example, should intruders compromise OS level security, all they see are encrypted files. This type of security protects against security breaches from the inside, for instance, by an administrator with malicious intent.

Encryption can be applied selectively by the file store, which makes it possible to have encrypted and unencrypted files in the same repository served by the same Documentum Content Server. TCS uses the 3DES-CBC encryption algorithm with a 192-bit key length. EMC licenses all encryption algorithms from RSA Security.

Encryption occurs within Documentum Content Server “below the API,” which means that content is exposed through the Documentum API in its unencrypted form. All applications access encrypted content without decoding—as if no encryption were applied. Indexing and full-text search are not impacted by encryption.

Repository encryption also applies to any backup conducted at the file system level. As a result, backup media can be safely stored without danger of a security breach. EMC NetWorker[®] for Documentum, for example, enables the backup and restoration of encrypted files from backup tapes containing encrypted data. Repository encryption is applied only to content files, not to its metadata (content properties). Nevertheless, since metadata is kept in a standard relational database, any RDBMS security measure provided by the database vendor can be employed. Oracle, for example, provides a complete database encryption solution.

All encryption comes with a performance trade off. The measured performance degradation of Documentum Content Server using encryption is less than 12 percent. Any additional performance degradation caused by audit logs, method executions, and other events is negligible. The security benefits of TCS, however, are substantial:

- Content security even if OS security is compromised
- Protection against “rogue” administrator
- Secure storage of backup media off site
- Secure backup media disposal

Electronic signatures

TCS enables any content asset or any content event such as a business process task to be signed electronically. Electronic signatures are securely linked to the content object and stored in the Documentum

repository as part of the audit trail. Any subsequent modification of the content invalidates the stored signature.

Signatures are date and time-stamped and include the name and password of the person signing and a justification for the signature. Each signature also contains a hash-checksum that verifies the authenticity of signed content. Only valid signatories are permitted to enter an electronic signature. The act of signing can enforce justification codes that are compliant with FDA 21 CFR Part 11 requirements. The signature manifestation in the viewed or printed document is compliant with those requirements. This is accomplished by a PDF manipulation tool that compares a set of strings representing signatures with a template that determines where these signatures need to be placed.

Documentum also provides the foundation for legally admissible digital signatures. A digital signature is a data element that allows the recipient of a message or transaction to verify its content and signatory. It's the electronic equivalent of having a paper document signed and notarized, but it is not a digitized image of a handwritten signature ("wet signature"). Users are validated using strong authentication (i.e. PKI cryptography) instead of just a login/password pair. Digital signatures are portable and can be verified outside of a signer's organization or location. When users choose to "digitally sign" a document, they are presented with an interface displaying a "Legal Notice," a drop-down list of justifications for performing the selected action, and user verification form.

Multi-dimensional access control

Documentum uses ACLs to manage access to content assets and other objects. Multi-dimensional access control provides the flexibility to grant access privileges based on group membership, which can represent any contextual information such as a user's role, location, means of access, IP address, or other criteria validated by the application.

For specific content, users may be required to belong to a certain group before being granted access, even though their normal access level would grant access by default. This feature enables security classifications such as "CLASSIFIED" or "TOP SECRET." Using such classifications, applications can limit access to content for specific individuals within a group even if the group as a whole would normally have access.

Multi-dimensional access control works by combining various ACLs to tighten the control administrators have over content access. In government, for example, only users with "top secret" clearance would have access to top secret documents. This clearance could vary depending on context—someone with top secret clearance who is accessing a document from outside the United States would also have to prove U.S. citizenship, which it is the job of the application to verify. That access might vary from "write" if the request originated from the U.S. to "read" if it originated from a hostile region.

By using logical combinations, mandatory rules may combine membership in various groups and non-membership in other groups. For example, access might be restricted to people who are members of both the Operation Staff and Vice Presidents groups, who are also members of either the Executive Vice Presidents or Officers groups, and not members of the Sales or Customer Service groups.

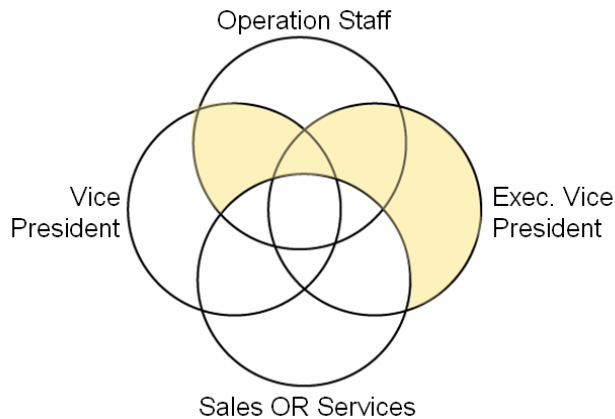


Figure 4. Multi-dimensional access control enables creation of complex access rules such as this example from corporate mergers and acquisitions.

Digital shredding

Many end users do not realize that when they delete their files, the files are not really gone. Deleted files may be recovered by analyzing the magnetic traces data leaves behind on its storage medium. This is how the FBI retrieves data from subpoenaed computers.

Digital shredding permanently destroys file data when the OS delete/unlink command is issued. It automatically writes over the location of data multiple times to ensure that it cannot be recovered, even by analyzing residual magnetism. This feature of TCS supports records management and retention policy applications that define when in its lifecycle content should be disposed. Documentum provides digital shredding for content stored in file systems as well as content addressed storage based on EMC Centera™. Digital shredding is considered a mandatory step for most records management applications.

Information rights management

The enterprise must reach beyond itself to enable vendors, distributors, contractors, regulators, and other partners to share unstructured information across the entire value chain. To be effective, it needs to control how content is viewed, printed, copied, and forwarded, and by whom. Ensuring security of content once it leaves the repository is a challenge. Even the most confidential contract or product plan may be compromised once it has been opened on a desktop, e-mailed, or printed. That's where EMC Documentum Information Rights Management (IRM)—also generically called digital rights management (DRM)—comes in.

The Documentum IRM Server and the various client components form a system with the primary objective of providing strong, persistent security and control over information in electronic form outside the repository. IRM advances the security of your Documentum repository in two fundamental ways. Firstly, it extends the access controls governing content inside the repository to follow the content wherever it goes outside the repository. Secondly, it extends the types of permissions that can be enforced on content to include control over the ability to print, copy, modify local copies, apply visual watermarks, and prevent screen capture. It accomplishes this through the use of strong cryptography, controlling access to decryption keys, and locking down viewing applications to prevent undesired use of the information once decrypted.

IRM system overview

The Documentum IRM architecture is made up of a family of client applications or plug-ins that work with a common policy server to secure and control electronic information. When information owners want to secure and control content, they start by “registering” that content with a Documentum IRM server. This can be initiated natively within the respective client application (e.g. Microsoft Office), in batch mode, or accomplished automatically by the Documentum system by virtue of the content being placed in an IRM-enabled folder or by the progression through a workflow or lifecycle state change. Once the content is registered (encrypted), it can be distributed safely through whatever mechanism or protocol is most appropriate. It is not necessary for the communication path to be secure since the content is intrinsically secure, though a secure path can be used for additional security measures.

When a recipient tries to open the protected content, the appropriate Documentum IRM client plug-in is automatically invoked. The plug-in establishes a secure connection back to the Documentum IRM server that holds the decryption keys. The recipient is authenticated over this connection and a request is made for the key to decrypt the content. When accessed in the context of a Documentum session, single sign-on can be leveraged to avoid multiple login prompts. Likewise, the IRM server can use the current Documentum ACLs to determine authorization. If the recipient is authorized, the server sends the key and use restrictions to the plug-in over the secure connection. The plug-in then locks down the viewing client, decrypts the content, renders it to the screen, and immediately destroys the decrypted content and its copy of the key. In this way, the system can dynamically enforce changes in policy, permissions, and group memberships in real time to content that has already left the protective confines of the Documentum repository. All activity involving protected content outside the repository is accessible through the standard Documentum user interfaces.

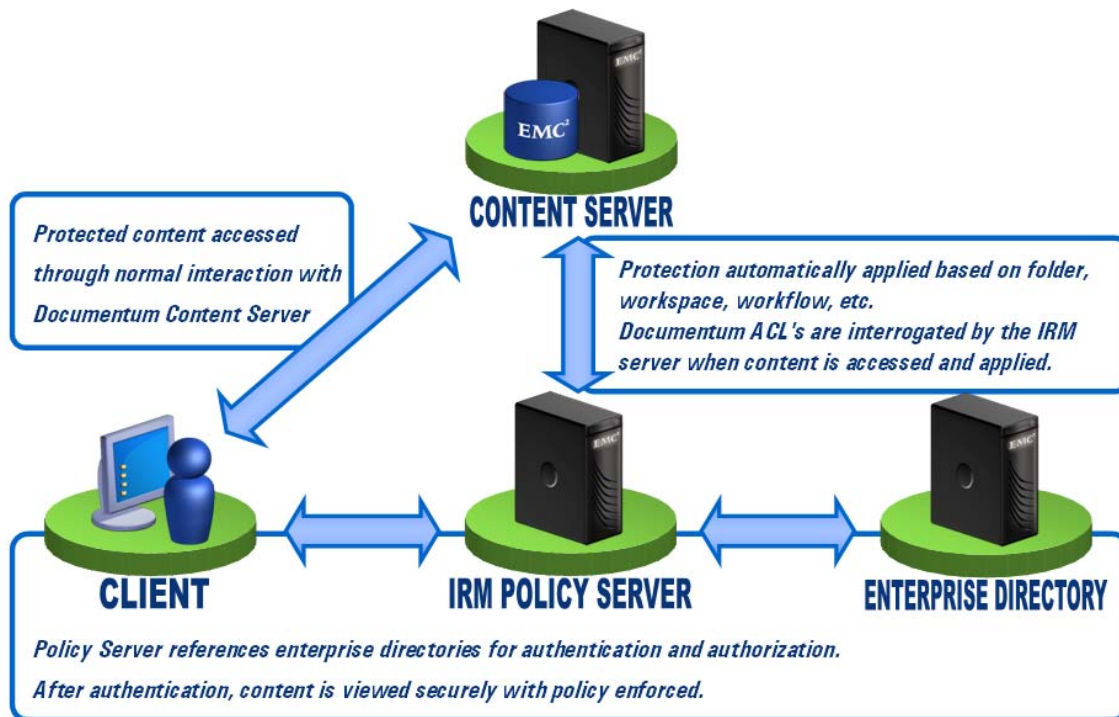


Figure 5. Permissions for access to content outside the Documentum repository can be set using standard Documentum clients and applications.

Abilities of Documentum IRM include:

-
- Determining who can access a document outside the repository
 - Prevention of documents from being forwarded to unauthorized e-mail recipients
 - Prohibiting the printing of an entire document or selected portions
 - Disabling of copy/paste and screen capture capabilities
 - Watermarking pages if printing privileges are granted
 - Expiring or revoking document access after distribution
 - Tracking all activities through a complete audit trail

In addition to the Documentum IRM solution, Documentum provides an IRM framework to integrate with other IRM/DRM vendors. Multiple IRM solutions can co-exist within the same Documentum installation, allowing customers to select best-of-breed technology that meets the needs of their business and their file types.

Common Criteria Certification

Established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), Common Criteria Certification is a program that evaluates IT product conformance to international security standards. The program to evaluate adherence to Common Criteria is known as the Common Criteria Evaluation and Validation Scheme (CCEVS). Compliance is accomplished first by evaluation of a product's security features by an accredited commercial testing lab using the Common Evaluation Methodology, followed by independent validation of the evaluation results by the National Information Assurance Partnership (NIAP).

The NIAP-CCEVS Validation Body assesses the results of security evaluations and issues Common Criteria certificates to those meeting the criteria. The certificate, along with the validation report, demonstrates conformance to the Common Criteria. The security features of EMC Documentum Content Server v5.3 and Documentum Administrator v5.3 were successfully validated on December 21, 2005, achieving Evaluation Assurance Level 2 (EAL2) conformance.

The NIAP-CCEVS Validation Body maintains a Validated Products List (VPL) of all IT products that have successfully completed evaluation and validation under the scheme. The list can be viewed online at the NIAP website, <http://www.niap-ccevs.org/>

DBSign for Client/Server Applications Version 3.0	9501	Gradkell Computers, Inc. Grady Gaston, VP 866-GRADKELL (866-472-3535) ext 18 ggaston@gradkell.com	EAL2	Sensitive Data Protection	30-Sep-2005
DBSign for HTML Applications Version 3.0	9502	Gradkell Computers, Inc. Grady Gaston, VP 866-GRADKELL (866-472-3535) ext 18 ggaston@gradkell.com	EAL2	Sensitive Data Protection	30-Sep-2005
DBSign for Oracle Web Forms Applications Version 3.0	10004	Gradkell Computers, Inc. Grady Gaston, VP 866-GRADKELL (866-472-3535) ext 18 ggaston@gradkell.com	EAL2	Sensitive Data Protection	30-Sep-2005
Delta Security Technologies Sentinel Model III Computer Security System	1000	Delta Security Technologies	EAL4	Sensitive Data Protection	13-Sep-2002
DiamondTEK Product (DiamondCentral: NSC Application SW (DiamondCentral, DiamondCentral Version 2.1.4, NSC (DiamondLink, DiamondPak, DiamondVPN) FW version 2.1.4)	4006	CryptTek, Inc.	EAL4	Firewall, VPN	28-Jun-2002
Documentum Content Server V5.3 and Documentum Administrator V5.3	10014	EMC, Documentum Division Jamal Shakra 925-600-6800 jamal.shakra@documentum.com	EAL2	Sensitive Data Protection	21-Dec-2005
FDREASE, Version 5.4, Level 50 • Addendum: Innovation Data Processing, FDRERASE IAERS 1.0	10084	Innovation Data Processing Thomas J. Meehan 973-900-7200 tmeehan@drinnovation.com	EAL2 Augmented with ADV_SPM.1, ALC_FLR.2	Sensitive Data Protection	29-Jul-2005
Finjan Software Incorporated, SurfinGate Version 5.6	4005	Finjan Software Incorporated Donna St John, Director of Marketing 732-556-1200 donna@finjan.com	EAL3	Sensitive Data Protection	31-Oct-2001

Figure 6. Documentum Content Server v5.3 and Documentum Administrator v5.3 have achieved Evaluation Assurance Level 2 (EAL2) validation by the NIAP-CCEVS Validation Body.

EMC Documentum—Delivering security you can trust

The Documentum enterprise content management platform provides the most secure content management infrastructure available today—which means no matter how demanding your security environment may be, Documentum is up to the challenge. With robust security features such as authentication, authorization, auditing, and encrypted data traffic built into Documentum Content Server, your most valuable information assets are well protected. Plus, Documentum Trusted Content Services delivers the additional data privacy capabilities necessary for even the most security conscious corporations and government agencies.

To fully leverage the enterprise benefits of content management, you need a content infrastructure that is secure at the core. You need Documentum enterprise content management.

About EMC

EMC Corporation (NYSE:EMC) is the world leader in products, services, and solutions for information storage and management. Through information lifecycle management (ILM) strategies, EMC helps enterprises of all sizes manage their growing volumes of information—from creation to disposal—according to its changing value. EMC information infrastructure solutions are at the heart of this mission, helping organizations manage, use, protect, and share their information assets more efficiently and cost-effectively. The result? Information with greater business value and at lower management cost.