National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

EMC Documentum Content Server™ V5.3 and EMC Documentum Administrator™ V5.3

Report Number: CCEVS-VR-05-0135
Dated: 21 December 2005
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

TABLE OF CONTENTS

1 Executive Summary

This report documents the NIAP validator's assessment of the evaluation of the EMC Documentum Content Server™ V5.3 and EMC Documentum Administrator™ V5.3, a product of EMC, Documentum Division, Pleasanton, CA. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by the CygnaCom Solutions Security Evaluation Laboratory (CCTL), and was completed during October 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by CygnaCom Solutions. The evaluation determined that the product is both **Common Criteria Part 2 extended and Part 3 conformant**, and meets the assurance requirements of EAL 2. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific organizational security policies while countering specific threats.

EMC Documentum Content Server™ V5.3 and EMC Documentum Administrator™ V5.3 (hereafter Documentum Content Management System) is a data management and control application. The Target of Evaluation (TOE) was evaluated using the *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004 [CCV2.2], and the *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Evaluation Methodology, January 2004 [CEMV2.2]. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4]. The Security Target (ST) for Documentum Content Management System is contained within the document *EMC Documentum Content Server™ V5.3 and EMC Documentum Administrator™ V5.3 Security Target,* dated 18 October 2005 [ST]. The ST has been shown to be compliant with the *Specification of Security Targets* requirements found within Annex A of Part 1 of [CCV2.2].

The Documentum Content Management System is an all-software TOE. It consists of three components that comprise the TOE:

- Content Server provides a single repository for content and metadata. Content Server uses an extensible object-oriented model to store content and metadata in the repository. Everything in a repository is stored as objects. The metadata for each object is stored in tables in the underlying RDBMS. The content files are stored in the underlying Operating System file system.
- Connection Broker is a name server for the Content Server.
- Administrator allows an authorized administrator to monitor, administer, configure, and maintain the Content Server and repositories via a Web browser.

Aspects of the following security functions are controlled / provided by the TOE in conjunction with the IT environment:

- Object access control
- Role-based user privileges
- Audit

The following are explicitly excluded from the TOE configuration, but are included in its environment:

- Client interface
- Hardware platforms and Operating Systems
- Database servers
- Cryptographic services of the operating system (SSL); and
- Network hardware and software (e.g., firewalls and routers)

The environment is assumed to counter the threats of unauthorized access to the physical components of the TOE. The operating system is assumed to properly authenticate users and protect files.

All copyrights and trademarks are acknowledged.

2 Identification

TOE: EMC Documentum Content Server^{TM} V5.3,
Connection Broker, and
EMC Documentum Administrator^{TM} V5.3

Evaluated Software: EMC Documentum Content Server^{TM} V5.3 (build # 5.3.0.115), and
EMC Documentum Administrator^{TM} V5.3 (build # 5.3.0.041 with CC Update #103292)

Developer: EMC Documentum
Pleasanton, CA

CCTL: Cygnacom Solutions' Security Evaluation Laboratory
Suite 5200
4925 Jones Branch Drive
McLean, VA 22102-3305

Validation Team: Edward A. Schneider (Institute for Defense Analyses)

CC Identification: *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004 [CCV2.2].

CEM Identification: *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Evaluation Methodology, January 2004 [CEMV2.2].

Interpretations: All NIAP and CCIMB interpretations as of the date of the Kick-off meeting held on 14 July 2004 were considered during the evaluation (all CCIMB interpretations issued prior to January 2004 had been incorporated into the version of the CC that was used). The interpretations listed below had a direct impact on the work performed.

Interpretations

Interpretation	Description	Affected Requirements
International Interpretations		
INTERP-137	Rules governing binding should be specifiable	FIA_USB

3 Security Policy

The EMC Documentum security policy is reflected in the security functional requirements for the TOE described in section 5.2 and 6.1 of the ST and for the IT environment described in sections 5.3 of the ST. A description of the principle security policies is as follows:

- **Identification and authentication:** The TOE requires users to be identified and authenticated before being allowed access to the system. However, this is done by the underlying operating system, which is part of the IT environment.

- **Object access control:** The EMC Documentum Content Server controls access to objects based on a subject's user name or group. An Access Control List associates user names and groups with an access level. An entry allows a user or group access up through a level or prohibits it above a level. There are also several extended permissions that may be explicitly allowed or prohibited. The access levels and extended permissions are specified in section 6.1.3 of the ST. Note: these controls are only in effect when repository security is on, which is the configuration that was evaluated.

- **Role-based user privileges:** The EMC Documentum Content Server supports three roles: SuperUser, Sysadmin, and User. A User may additionally have privileges Create Type, Create Cabinet, and Create Group. In addition, there are extended privileges Config audit, Purge audit, and View Audit. Tables 5-2 and 5-3 and Section 6.1.3 of the ST describes what these roles and privileges allow a user to do.

- **Audit:** The TOE provides an auditing capability, although the audit records are stored in a database external to the TOE. Significant auditable events are:

  - user login failure,
  - all operations performed on objects,
  - all operations performed in repository,
  - administrative actions performed.

The security functional requirements for the TOE and the IT environment are documented in section 5 of the ST. A combination of requirements drawn from part 2 of the CC [CCV2.2] and explicitly stated security requirements were necessary due to the reliance of the TOE on the IT environment to protect audit records and to prevent activities outside the control of the TOE from the TSF. A summary of the SFRs for the TOE and IT environment are included in the tables below.

TOE Security Functional Requirements

Class FAU: Security Audit	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG_EXP.1	Protected audit trail storage
Class FDP: User Data Protection	
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_USB.1	User subject binding
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of the TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Class FPT: Protection of the TSF	
FPT_RVM_EXP.1-1	Non-bypassability of the TSP
FPT_SEP_EXP.1-1	TSF domain separation

IT Environment Security Functional Requirements

Class FAU: Security Audit	
FAU_STG_EXP.1-2	Protected audit trail storage
Class FIA: Identification and Authentication	
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
Class FPT: TOE Protection	
FPT_RVM_EXP.1-2	Non-bypassability of the TSP
FPT_SEP_EXP.1-2	TSF domain separation
FPT_STM.1	Reliable time stamp

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements:

ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

4.2 Environmental Assumptions

The environmental assumptions listed in the following table are required to ensure the security of the TOE.

Environmental Assumptions

Assumption	Description
A.Admin	The authorized administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.
A.Database	The IT environment provides a database to store TSF data.
A.NoUntrusted	There are no untrusted users and no untrusted software on the Documentum Content Server host.
A.OS	The OS provides file protection and user authentication.
A.Physical	The TOE components critical to the security policy enforcement will be protected from unauthorized physical modification by being located within controlled access facilities and behind a Firewall.
A.ProtectComm	Those responsible for the TOE will ensure the communications between the Documentum Administrator and Documentum Content Server host are secure.
A.Time	The underlying operating system provides reliable time stamps.

4.3 Clarification of Scope

The Documentum Content Management System executes on top of third-party operating systems and uses third-party databases to store audit and other administrative data and managed content. A process running with root privilege on the operating system can bypass all of the TOE security controls. Thus, non-bypassability of the TOE Security Policy and Domain Separation are limited to those instances when the operating system invokes the TOE Security Function. Likewise, the TOE relies on the underlying operating systems to provide secure and reliable communication between its components.

Documentum clients interact with the system through a GUI that is installed on their workstations and that sends messages through the Connection Broker. This GUI is not part of the TOE and client interface documentation is not part of the TOE documentation considered in this evaluation.

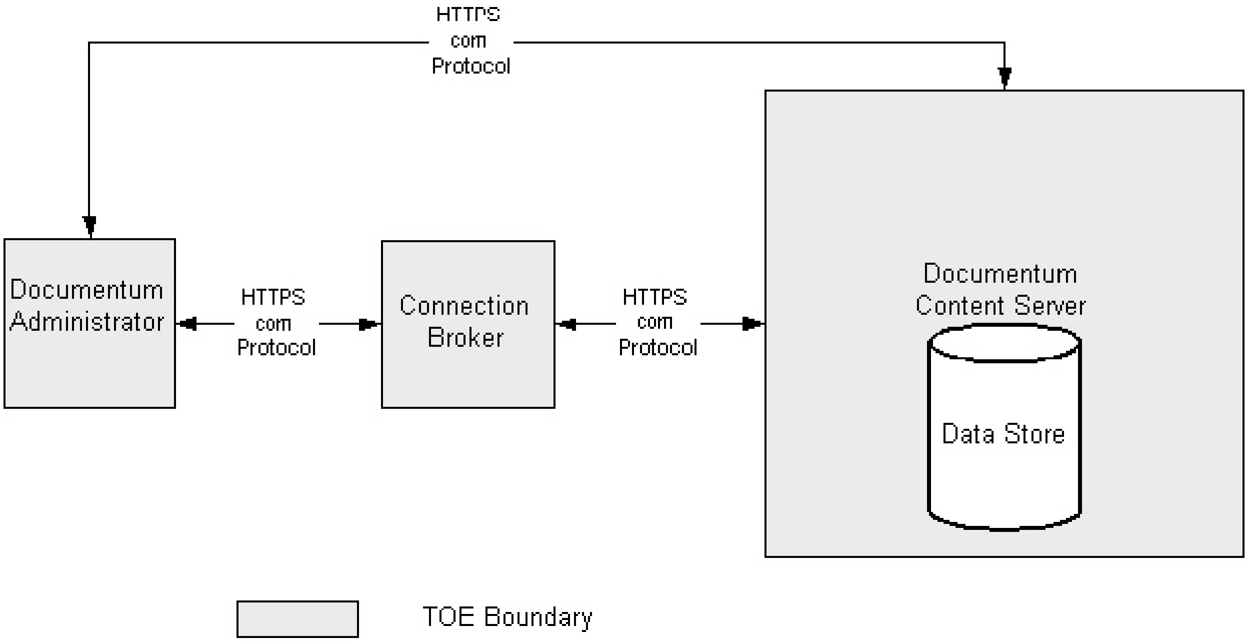
There are two ways for a purchaser to obtain the TOE: on a CD or by downloading an install package from www.intraware.com. Only the downloaded version was evaluated and this method must be used.

5 Architectural Information

Documentum is a content management system, consisting of a Content Server, a Connection Broker, and a Documentum Administrator. The Documentum Content Server is the core functionality that allows users to create, capture, manage, deliver, and archive enterprise content data. Content data is the actual data managed by the Content Server. Metadata is the attributes of the data. The functionality and features of Documentum Content Server provide the management and security of content data and metadata in the repository; it was evaluated on Microsoft Windows Server 2003 with an Oracle database. The Connection Broker is a name server to a particular repository. The Documentum Administrator is the administrator interface; it was evaluated on Microsoft Windows Server 2003 using Internet Explorer.

The Client interface is not part of the TOE. Likewise, the underlying operating systems, databases, web browsers and the communication protocols linking distributed elements of the architecture are not in the TOE.

An architectural diagram of the TOE.



6 Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- EMC Documentum Content Server^{TM} V5.3 and EMC Documentum Administrator^{TM} V5.3 Security Target.
- Documentum Administrator User Guide V5.3.
- Content Server Administrator's Guide V5.3.
- Content Server Fundamentals V5.3
- Content Server API Reference Manual V5.3
- Content Server Installation Guide V5.3
- Content Server and Documentum Administrator v5.3 Configuration Management Capabilities
- Documentum Content Server V 5.3 and Documentum Administrator V5.3 Common Criteria Supplement Guide
- Web Development Kit and Applications Installation Guide V 5.3

7 IT Product Testing

7.1 Developer Testing

The vendor testing covered all of the security functions identified in Section 6.1 of the ST. These security functions were: Security Audit, Managed User Access, and Security Management. At EAL2, vendor testing must demonstrate correspondence between the tests and the functional specification. However complete testing is not required; "coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested."[1]

The testing was focused on demonstrating that the SFRs worked as claimed in the ST. The test procedures consisted mainly of automated scripts, with a few manual tests to test administrator operations entered through the Administrator component. For the automated scripts, the output from the script was stored in a file and then compared with the expected results file. For the manual tests, a screen shot showing the results was saved.

The testing showed that the proper audit records were generated and contained the required information, that authorized administrators could access the audit records, and that unauthorized users could not. It also tested both authorized and unauthorized accesses to the stored content.

The evaluator determined that the vendor tested (at a high level) most of the security-relevant aspects of the product that were claimed in the ST. The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluators determined that the developer's approach to testing the TSFs was appropriate for this EAL2 evaluation.

7.2 Evaluator Independent Testing

At EAL 2, the stated purpose of the evaluator's independent testing activity "is to determine, by independently testing a subset of the TSF, whether the TOE behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests." (CEM 6.8.4.1). The CEM further instructs the evaluator to consider a number of factors including: the "Rigour of developer testing of the security functions. Some security functions identified in the functional specification may have had little or no developer test evidence attributed to them." (CEM 6.8.4.3.2) As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

The evaluation team installed the TOE as specified in the secure installation procedures. The same test equipment that was used for developer testing was used for the independent testing, except that the Administrator was installed on a separate hardware platform from the rest of the TOE to verify proper functioning in a distributed environment. Both platforms were Pentium-based machines and were connected via SSL. The Connection Broker and the Oracle database

[1] CEM, V2.2, paragraph 6.8.2.2 (application note for EAL2:ATE_COV.1)

were installed on the Content Server host. There were two repositories on the Content server: one for testing the Content Server functionality and another for testing the Administrator functionality, and one instance of the Oracle database.

The evaluator reran all of the automated scripts and several of the manual tests. All of the results duplicated those of the developer. The evaluator also devised seven tests, each of which covered multiple security functionalities. The first test created all types of users, covering all possible permissions. The subsequent tests used these users to perform many of the allowed and disallowed functions for the users. Some tests were devised to test boundary conditions. Both positive and negative tests were devised. Each of these tests produced the expected results.

Test results, which are contained in proprietary reports, were satisfactory to both the Evaluation Team and the Validation Team.

7.3 Strength of Function

There are no specific SOF claims pertaining to a specific IT Security Function(s) since Identification and Authentication is done in the environment.

7.4 Vulnerability Analysis

The vendor searched for publicly known vulnerabilities specifically related to the TOE using key words related to the product type, as well as publicly known vulnerabilities in the third-party products that are incorporated in the TOE. No publicly-known vulnerabilities specific to the evaluated version of Documentum were found. The developer examined the known vulnerabilities in the supporting third party products (MS Windows, Oracle database, Internet Explorer) using the National Vulnerability Database (nvd.nist.gov), the Common Vulnerability and Exposure list (www.cve.mitre.org), and SecureFocus (www.securityfocus.com); an explanation was given why these are not exploitable in the intended environment.

The evaluator devised penetration tests using the developers analysis, including some of the developer's tests. NESSUS (www.nessus.org) was used for port analysis. No exploitable obvious vulnerabilities were found.

8 Evaluated Configuration

The evaluated configuration was EMC Documentum Content Server^{TM} V5.3 (build # 5.3.0.115), and EMC Documentum Administrator^{TM} V5.3 (build # 5.3.0.041 with CC Update #103292).

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC, Version 2.2; CEM, Version 2.2, and all applicable NIAP CCEVS and International Interpretations in effect on 14 July 2004.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The evaluation determined that the product is both **Common Criteria Part 2 extended and Part 3 conformant**, and meets the assurance requirements of EAL 2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom Solutions. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

10 Validator Comments/Recommendations

The Validator agrees with the conclusion of the CygnaCom Solutions Evaluation Team, and recommends to CCEVS Management that an EAL2 certificate rating be issued for EMC Documentum Content Server^{TM} V5.3 and EMC Documentum Administrator^{TM} V5.3.

The evaluators have looked at the design of the Content Server and Administrator, tested their functionality, and looked for obvious vulnerabilities; they found that the TOE satisfies the functional claims made in the ST and the validator concurs. Note that no evaluation verifies that there are no flaws, only that the evaluator could not find any.

The TOE does not protect the connection between itself and the Client interface; an unauthorized party could potentially observe this connection. As recommended by EMC Documentum, the TOE and the Client should be installed such that interactions are protected by SSL. Also, a firewall should be installed to protect against unauthorized access to the TOE.

The TOE is a software application that sits on top of a commercial operating system and that interacts with commercial databases. It depends on these to protect itself and its data from unauthorized access, such as installing a virus into the Content Server code. Any patches for these products should be promptly installed.

11 Security Target

The Security Target for EMC Documentum Content Server^{TM} V5.3 and EMC Documentum Administrator^{TM} V5.3 is contained within the document *EMC Documentum Content Server^{TM} V5.3 and EMC Documentum Administrator^{TM} V5.3 Security Target,* dated 8 December 2005. [ST]. The ST is compliant with the *Specification of Security Targets* requirements found within Annex A of Part 1 of the CC [CCV2.2].

12 Glossary

The following table is a glossary of terms used within this validation report.

Acronym	**Expansion**
CC	*Common Criteria for Information Technology Security Evaluation*. [Note: Within this Validation Report, CC always means Version 2.2, dated January 2004.]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CCIMB	Common Criteria Interpretations Management Board
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
I&A	Identification and Authentication
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profile
SFR	Security Function Requirement
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): http://niap.nist.gov/cc-scheme/
- Cygnacom Solutions: http://www.cygnacom.com/
- EMC Documentum: http://www.documentum.com/

CCEVS Documents

[CCV2.2] *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004.

[CEMV2.2] *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Part 2: Evaluation Methodology, January 2004.

[CCEVS3] *Guidance to Validators of IT Security Evaluations*, Version 1.0, February 2000.

[CCEVS4] *Guidance to Common Criteria Testing Laboratories*, Draft, Version 1.0, March 2000.

Other Documents

[ST] *EMC Documentum Content Server^{TM} V5.3 and EMC Documentum Administrator^{TM} V5.3 Security Target*, Version 2.0, 8 December 2005.