Certification Report

EAL 2 Evaluation of EMC® Corporation's

EMC® Smarts® Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-65-CR
Version:	1.0
Date:	03 August 2007
Pagination:	i to v, 1 to 13

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 03 August 2007.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked or registered trademarks:

- Smarts is a registered trademark symbol of EMC Corporation.
- EMC is a registered trademark symbol of EMC Corporation.
- Codebook Correlation Technology and Common Information Model are trademarks of EMC Corporation.
- Microsoft, and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- CVE is a trademark of MITRE Corporation.
- Intel and Pentium are registered trademarks of Intel.
- JAVA and Java Runtime Environment (JRE) are registered trademarks of SUN Microsystems, Inc.
- Linux is a registered trademark of Linus Torvalds. Inc.
- Red Hat is a registered trademark of Red Hat, Inc.
- SANS is a trademark of SANS/ESCAL.
- Sun and Solaris are trademarks of Sun Microsystems, Inc. in the United States and other countries.
- UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

The EMC® Smarts® Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1, from EMC® Corporation (hereafter referred to as EMC® Smarts® Suite) is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The EMC® Smarts® Suite is a collection of software products which monitor IT networks. It can map networks, monitor the availability and performance of network nodes, and show the business implications of any failures. EMC® Smarts® Suite consolidates network events and presents them at a suitable level of abstraction to allow administrators to prioritize problems according to business impact and helps administrators to distinguish the root cause of a problem from the collateral impacts.

Electronic Warfare Associates-Canada, Ltd. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 28 June 2007 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the EMC® Smarts® Suite, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 2 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

The Communications Security Establishment, as the CCS Certification Body, declares that the EMC® Smarts® Suite evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) at http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official International Common Criteria Program website at http://www.commoncriteriaportal.org.

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation is the EMC® Smarts® Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1, from EMC® Corporation (hereafter referred to as EMC® Smarts® Suite).

2 TOE Description

The EMC® Smarts® Suite is made up of 3 monitoring components and a discovery component which map and monitor IP networks and critical servers, and then pass information on availability and performance about the IP networks and critical servers to the core management server, which aggregates this information and presents it to the user through the Global Console or the web browser. Other modules provide additional capabilities to calculate and display the business impact of infrastructure problems and to produce a wide variety of reports. A broker manages a registry of EMC® Smarts® server applications, which allows each component to discover other components of the system.

EMC® Smarts® Suite helps system administrators cope with the flood of raw events which will be generated by a problem in the IT infrastructure. The system uses a normalized event reporting structure, which identifies and consolidates duplicated events.

The EMC® Smarts® Suite can also distinguish between the root cause of problems and collateral impacts. For example, one router failing might increase the throughput of other routers and cause them to fail. The system administrator will receive events from many routers, but only needs to address the problem on one router. The system uses patented Codebook Correlation Technology; this set of algorithms computes a correlation between the set of possible symptoms and the root cause that can best explain the symptoms, based on the nature of the symptoms and the network topology. The processing of these algorithms is distributed throughout the system for optimal performance, but the final correlation analysis, policy implementation, and presentation to the user occurs in the core management server.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the EMC® Smarts® Suite is identified in Section 5 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature: Title: EMC Corporation EMC® Smarts® Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1, Security Target, Version: 0.6, Date: 26 June 2007.

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

The EMC® Smarts® Suite is:

a. Common Criteria Part 2 conformant; with functional requirements based only upon functional components in Part 2;
b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c. Common Criteria EAL 2 conformant, with all the security assurance requirements in the EAL 2 package.

6 Security Policy

The following statements are representative of the Security Policy:

Authentication and Security Management. Users must authenticate to the EMC® Smarts® Suite to be able to access its security functions, event data, and audit data. A user authenticating to the EMC® Smarts® Suite must provide a user name and password for a valid user account. The EMC® Smarts® Suite implements role-based security management. A role is assigned to an administrator when the administrator account is created. Login is not permitted if there is no associated role for the administrator.

Protection of Data Transmitted Between TOE Components. All TOE Security Function data communicated between the physically-separated components of the EMC® Smarts® Suite of software components is protected from disclosure by using direct protection via EMC Corporation's implementation of AES[1]. The key is derived from a Diffie-Hellman exchange.

For security policy enforcement please refer to the EMC® Smarts® Suite Security Target.

[1]**NOTE:** Assessment of EMC Corporation's AES implementation did not form part of this CC evaluation and was not separately validated under the Cryptographic Module Validation Program.

7 Assumptions and Clarification of Scope

Consumers of the EMC® Smarts® Suite product should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage assumptions are listed in the ST:

- There will be one or more appropriately trained individuals assigned to manage the EMC® Smarts® Suite and the security information it contains; and
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the EMC® Smarts® Suite documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The host machine(s) upon which EMC® Smarts® Suite is installed resides in a physically secure location and only authorized individuals are granted physical access to the host; and
- The EMC® Smarts® Suite will be installed and connected at all times to the network it is intended to monitor.

For more information about the EMC® Smarts® Suite security environment, refer to Section 3 of the ST (TOE Security Environment).

7.3 Clarification of Scope

The EMC® Smarts® Suite is intended for use by a non-hostile and well-managed user community. It relies on the environment to provide it physical and logical protection.

8 Architectural Information

EMC® Smarts® Suite includes the following products:

- Service Assurance Manager – the core management server for the whole system
- Global Console – the primary interface to the Service Assurance Manager

- Business Impact Manager – extends the capabilities of Service Assurance Manager by calculating the business impact of events.
- Business Dashboard – extends the capabilities of Service Assurance Manager by presenting the business impacts of events.
- Report Manager – extends the capabilities of Service Assurance Manager by storing events in a database ready to compile into reports.
- Discovery Manager – discovers and presents the topology of Internet Protocol (IP) networks.
- IP Availability / Performance Manager – monitors the availability and performance of IP networks.
- Server Performance Manager – monitors the performance of critical servers.
- Broker – manages a registry of EMC® Smarts® server applications.

EMC® Smarts® **Service Assurance Manager** primary tasks is topology and event consolidation. **Service Assurance Manager** imports infrastructure elements (such as hosts and routers) and applications from each underlying managed domain. As it imports the elements, it consolidates elements that are reported by different sources. **Service Assurance Manager** also imports the relationships between the elements from the underlying managed domains. Using these relationships and overlapping devices, **Service Assurance Manager** accurately pieces together a complete topology of the managed environment. Notifications received from multiple sources are consolidated into single events. Similarly, impacts reported by different sources for the same problem are consolidated and associated with the event in **Service Assurance Manager**.

The EMC® Smarts® **Service Assurance Manager** classifies notifications according to their calculated severity. The following levels are used:

- Critical: identifies a specific failure that requires resolution.
- Major: identifies a serious condition that requires immediate attention.
- Minor: identifies an abnormal condition that is not serious but requires some action.
- Unknown: identifies an unknown, unreachable, disconnected, or suspended condition.
- Normal: the element is in its normal state.

Escalation policies enable EMC® Smarts® administrators to automate responses to events.

An audit log entry is associated with each of the notifications that the EMC® Smarts® **Service Assurance Manager** receives from the underlying EMC® Smarts® applications. The audit log entry includes the following information:

- Event;
- Time of the update;
- Name of the operations person or system that made the update;
- Type of audit entry; and
- Description of the entry (Notify, Clear, or Suspend, for example).

The **Global Console** is a standalone Java program which runs on any system with Java Run-Time Environment (JRE) v1.4.2 or higher. It is the primary interface for all EMC® Smarts® administrators. EMC® Smarts® administrators use the **Global Console** to monitor EMC® Smarts® domains, acquire detailed information about topology and events, respond to problems, and take corrective action. EMC® Smarts® administrators with appropriate privileges can use the **Global Console** to discover topology, administer underlying domains, as well as administer EMC® Smarts® users, user profiles, program tools, and escalation policies.

EMC® Smarts® **Business Impact Manager** operates in conjunction with, and extends the capabilities of, EMC® Smarts® Service Assurance Manager to calculate the business impact of events. It then propagates the impacts to affected business elements (service offerings, business processes, and the users of the processes). The propagated impacts are discrete notifications that are connected through a causal event chain to the authentic problem(s) in the network infrastructure responsible for the problems of the business processes and elements. Each authentic problem includes a business impact value. The business impact value is displayed in the Notification Log of Service Assurance Manager. The Impacted instance of the business element displays a Severity Icon that is colored according to the severity level of the notification.

To perform its operations, **Business Impact Manager** includes facilities to import business element definitions. Additionally, **Business Impact Manager** includes a Topology Builder console through which business elements can be added and modified. **Business Impact Manager** also includes facilities to assign weights to business and infrastructure elements in the topology. **Business Impact Manager** uses the assigned weights when calculating values for business impacts.

The EMC® Smarts® **Business Dashboard** displays the results of EMC® Smarts® analysis in a flexible, Web-based user interface. The EMC® Smarts® **Business Dashboard** provides the views from the Global Console as individual components called dashboard viewlets. The user can configure the display and contents of viewlets to customize the presentation of EMC® Smarts® analysis, enabling delivery of role-based views of the managed topology across all layers of the IT environment.

While the Global Console is the primary user interface for EMC® Smarts® software, the EMC® Smarts® **Business Dashboard** provides another means of viewing and responding to the analysis provided by EMC® Smarts® Service Assurance Manager.

The **Report Manager** receives notifications of all events from the Service Assurance Manager and stores these events in a relational database in a schema customized for interoperability with third party reporting applications. EMC® Smarts® administrators at the Global Console can request reports to be produced. This initiates a query to the **Report Manager** that extracts notification information from the database. The reports are distributed by way of HTTP servers to end user web browsers.

The **Discovery Manager** uses Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) polling to collect topology information about the managed environment. Initially the **Discovery Manager** process pings the IP address of the discovery candidate system to see if the address is a reachable address. If the address is reachable, the discovery process sends an SNMP request to the system requesting the following system-related information:

- Description – a textual description of the entity;
- Object ID – an identification of the network the entity is on;
- Contact - identification of the contact person for this entity;
- Name - an administratively-assigned name for this entity. By convention, this is the fully-qualified domain name of the node; and
- Location - the physical location of this node.

The **Discovery Manager** uses this information to determine if the entity should be added to the topology map. For example, a router with two network cards might be discovered twice but would only be added once. If an entity is to be added the gathered information is used to determine its relationship with other elements of the topology.

The **IP Availability / Performance Manager** monitors the availability and performance of IP networks, at layers 2 and 3 of the Open Systems Interconnection (OSI) model by sending ICMP ping requests and SNMP v1, 2c and 3 polls. The polling interval and the actionable threshold setting are configurable.

The **Server Performance Manager** monitors the availability and performance of servers by sending ICMP ping requests and SNMP v1, 2c and 3 polls. The polling interval and the actionable threshold setting are configurable.

The **Broker** manages a registry of EMC® Smarts® server applications. Periodically, the **Broker** pings the applications in its registry to determine whether they are still active.

9 Evaluated Configuration

The EMC® Smarts® Suite Security Target defines the following systems in the evaluated configuration:

a. Service Assurance Management Suite; and

b. Internet Protocol Management Suite.

These components combine to form the evaluated configuration which operates on the following operating systems:

- Solaris 8 and 9
- HP-UX 11.11

- Windows 2000 Server and Windows 2003 Server (Service Pack 1)
- Red Hat Linux Advanced Server and Enterprise Server 3

The Global Console can operate on any system which supports the Java Runtime Environment v1.4.2 and supports the following browsers; Netscape 7.0 (or higher) and Internet Explorer 6.0 SP1 (or higher) with JavaScript enabled.

10 Documentation

The EMC® Corporation documents provided to the consumer are as follows:

a. EMC® Smarts® 6.5.1 System Administration Guide;
b. Service Assurance Manager 6.5.1 Dashboard Configuration Guide;
c. IP Management Suite 6.5.1 Deployment Guide;
d. IP Management Suite 6.5.1 Discovery Guide;
e. IP Management Suite 6.5.1 Installation Guide;
f. IP Performance Manager 6.5.1 Users Guide;
g. IP Availability Manager 6.5.1 Users Guide;
h. Service Assurance Manager 6.5.1 Operators Guide;
i. EMC® Smarts® 6.5.1 Quick Start Guide;
j. EMC Corporation EMC® Smarts® 6.5.1 Release Notes;
k. Service Assurance Manager 6.5.1 Configuration Guide;
l. Service Assurance Manager Suite 6.5.1 Deployment Guide;
m. Service Assurance Manager Suite 6.5.1 Installation Guide;
n. Service Assurance Manager 6.5.1 Introduction.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the EMC® Smarts® Suite, including the following areas:

Configuration management: An analysis of the EMC® Smarts® Suite CM system and associated documentation was performed. The evaluators found that the EMC® Smarts® Suite items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the EMC® Smarts® Suite during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the EMC® Smarts® Suite functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the EMC® Smarts® Suite administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Vulnerability assessment: The EMC® Smarts® Suite ST's strength of function claims were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability analysis and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer had met their testing responsibilities by reviewing the developer's test plan, test approach, test procedure and test results, and examining their test evidence, as documented in the Evaluation Technical Report (ETR)[2].

The evaluators analyzed the developer's test coverage analysis, and found that the correspondence between tests identified in the developer's test documentation and the functional specification was complete and accurate.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation,

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. These tests focused on:

- Identification and authentication;
- Audit;
- Security Management;
- Basic product functionality.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Generic vulnerabilities;
- Bypass attempts;
- Tampering; and
- Direct attacks.

The evaluator conducted a port scan of the EMC® Smarts® Suite. The only ports found to be open were ones that would be expected. The evaluator used a publicly available tool to scan the EMC® Smarts® Suite for weaknesses, and none were found. The evaluator also used a publicly available packet capture tool to examine output from the EMC® Smarts® Suite during startup, shutdown and normal operations. The evaluator searched the captured results in an attempt to extract information which might be useful to a potential attacker; no useful information was uncovered. In addition, the evaluator performed direct attacks on the EMC® Smarts® Suite, attempting to bypass or break the TOE’s role-based security mechanisms.

The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment.

12.4 Conduct of Testing

The EMC® Smarts® Suite was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the ITSET Facility at Electronic Warfare Associates-Canada, Ltd. The CCS Certification Body witnessed a portion of the independent testing.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the EMC® Smarts® Suite behaves as specified in its ST and functional specification. The penetration testing resulted in a **PASS** verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in the EMC® Smarts® Suite in its intended operating environment.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 2** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for the EMC® Smarts® Suite includes a comprehensive Installation and Users Guide.

The EMC® Smarts® Suite is straightforward to configure, use and integrate into a corporate network.

EMC® Corporation Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

EWA-Canada performed separate site visits to review developer processes (ACM, ADO, and ATE) and to repeat a sample of developer's tests. This is reported on in the CC Evaluation Site Visit Report.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme

Acronym/Abbreviation/ Initialization	Description
CPL	Certified Products list
CM	Configuration Management
CSE	Communications Security Establishment
DoD	Department of Defense
EAL	Evaluation Assurance Level
ECIM	EMC Common Information Model
ICMP	Internet Control Message Protocol
ETR	Evaluation Technical Report
IP	Internet protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
JRE	Java Runtime Environment
OSI	Open Systems Interconnection
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
SANS	SysAdmin, Audit, Network, Security
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
US-CERT	United States Computer Emergency Readiness Team

16 References

This section lists all documentation used as source material for this report:

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, version 2.3 Revision 326, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, version 2.3 Revision 326, August 2005.

d. EMC Corporation EMC® Smarts® Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1, Security Target, Version: 0.6, 26 June 2007.

e. Evaluation Technical Report (ETR) EMC® Smarts® Service Assurance Management (SAM) Suite and Internet Protocol (IP) Management Suite 6.5.1, EAL 2 Evaluation, Common Criteria Evaluation Number: 383-4-65, Document No. 1546-000-D002, Version 1.3, 28 June 2007.