Certification Report

EMC SourceOne™ v7.2

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-306-CR
Version: 1.0
Date: 11 January 2016
Pagination: i to iii, 1 to 10

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 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies 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, 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 Communications Security Establishment, 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.

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/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration 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 EWA-Canada.

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 11 January 2016, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademark:

- SourceOne is a trademark of EMC Corporation

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

TABLE OF CONTENTS

Executive Summary

EMC SourceOne™ v7.2, from EMC Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that EMC SourceOne v7.2 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

EMC SourceOne v7.2 is a software-based, distributed solution that archives content from email, file, and Microsoft SharePoint servers and provides role-based search and discovery capabilities. It is implemented as a collection of applications, processing services, databases, and archives running on Windows based systems. In the evaluated configuration, all of the TOE software components are running within a virtualized environment provided by VMware ESXi 5.0.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 11 January 2016 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 EMC SourceOne v7.2, and the security functional/assurance 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.

Communications Security Establishment, as the CCS Certification Body, declares that the EMC SourceOne v7.2 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) and the Common Criteria portal (the official website of the Common Criteria Project).

1   Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is EMC SourceOne™ v7.2, from
EMC Corporation.

2   TOE Description

EMC SourceOne v7.2 is a software-based, distributed solution that archives content from
email, file, and Microsoft SharePoint servers and provides role-based search and discovery
capabilities. It is implemented as a collection of applications, processing services, databases,
and archives running on Windows based systems. In the evaluated configuration, all of the
TOE software components are running within a virtualized environment provided by
VMware ESXi 5.0.

A diagram of the EMC SourceOne v7.2 architecture is as follows:
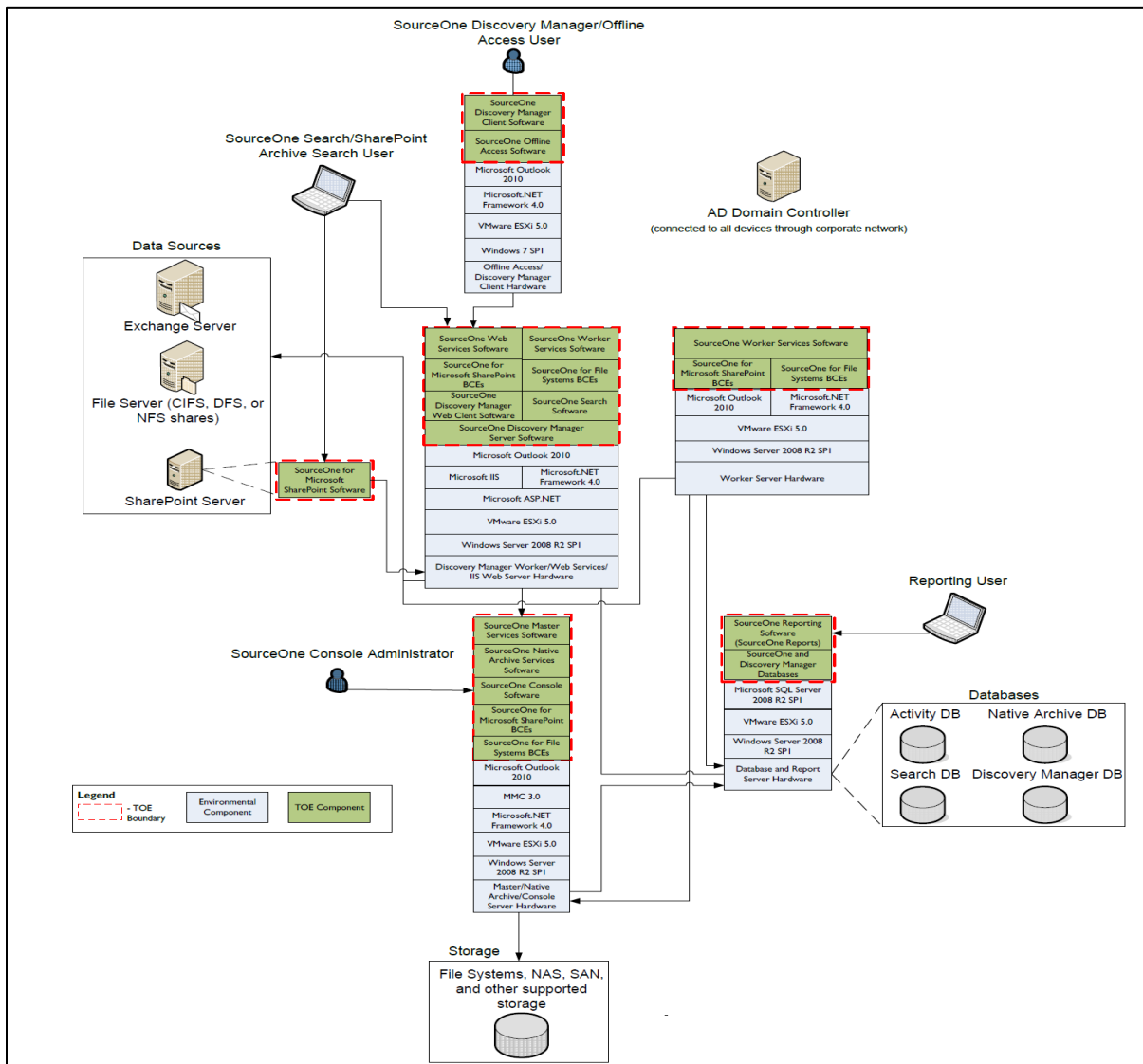
3   Security Policy

EMC SourceOne v7.2 implements a role-based access control policy to control administrative access to the system and user access to archived content. In addition, EMC SourceOne v7.2 implements policies pertaining to the following security functional classes:

- *Security Audit*
- *User Data Protection*
- *Identification and Authentication*
- *Security Management*
- *Protection of the TOE Security Functions*
- *Resource Utilization*

4   Security Target

The ST associated with this Certification Report is identified below:

EMC SourceOne File Systems v7.2, Email Management v7.2, Discovery Manager v7.2, and for Microsoft SharePoint v7.1 Security Target, Version 1.6, January 6, 2016.

5   Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

EMC SourceOne v7.2 is:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following: ALC_FLR.2 - Flaw Reporting Procedures,

b. Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2,

c. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of EMC SourceOne v7.2 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.*

- *The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE is installed on the appropriate, dedicated hardware and operating system.*

- *The TOE environment provides the network connectivity required to allow the TOE to perform its functions.*

- *The IT environment provides the TOE with the necessary reliable timestamps.*

- *The TOE is located within a controlled access facility.*

- *The TOE software will be protected from unauthorized modification.*

7   Evaluated Configuration

The evaluated configuration for EMC SourceOne v7.2 comprises the following software components:

- SourceOne Email Management v7.2 build 7.20.2524
    - SourceOne Console software
    - SourceOne Search software
    - SourceOne Master Services software
    - SourceOne Worker Services software
    - SourceOne Web Service software
    - SourceOne Native Archive Services software
    - SourceOne Reporting software
    - SourceOne Databases
    - SourceOne Discovery Manager Client software (automatically installed with SourceOne Email Management)
- SourceOne for Microsoft SharePoint v7.1 build 7.12.2075
    - SourceOne SharePoint Solutions
    - SourceOne for Microsoft SharePoint BCEs software
- SourceOne for File Systems v7.2 build 7.20.2524
    - SourceOne for File Systems BCEs software
- SourceOne Discovery Manager v7.2 build 7.20.2524
    - SourceOne Discovery Manager Client software
    - SourceOne Discovery Manager Web Client software
    - SourceOne Discovery Manager Server software
    - SourceOne Discovery Manager Database

In the evaluated configuration, all of the TOE software components are running on Windows-based platforms within a virtualized environment provided by VMware ESXi 5.0. The Source One Discovery Manager Worker/Web Services/IIS Web Server, Master/Native Archive/Console Server, Worker Server, and Database and Report Server operate with Windows Server 2008 R2 SP1. The Discovery Manager client host computer is a standard desktop with Windows 7 SP1. The evaluated configuration also includes Microsoft Exchange Server 2010 and SharePoint Server 2010.

The publication entitled EMC SourceOne File Systems v7.2, Email Management v7.2, Discovery Manager v7.2, Offline Access v7.2, and for Microsoft SharePoint v7.1 Guidance Documentation Supplement, Version 0.3 describes the procedures necessary to install and operate EMC SourceOne File Systems v7.2 in its evaluated configuration.

8   Documentation

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

a. EMC SourceOne Email Management 7.2 Installation Guide, Rev01;

b. EMC SourceOne Email Management 7.2 Administration Guide, Rev01;

c. EMC SourceOne 7.2 Search User Guide, Rev01;

d. EMC SourceOne Products Compatibility Guide, Rev47;

e. EMC SourceOne Email Management 7.2 Release Notes;

f. EMC SourceOne Discovery Manager 7.2 Installation and Administration Guide, Rev01;

g. EMC SourceOne Discovery Manager 7.2 Desktop User Guide, Rev01;

h. EMC SourceOne Discovery Manager 7.2 Web Application User Guide, Rev01;

i. EMC SourceOne Discovery Manager 7.2 Release Notes;

j. EMC SourceOne for Microsoft SharePoint 7.1 Installation Guide, Rev01;

k. EMC SourceOne for Microsoft SharePoint 7.1 Administration Guide, Rev01;

l. EMC SourceOne 7.2 for File Systems Administration Guide; Rev01;

m. EMC SourceOne for File Systems, Version 7.2, Installation Guide, Rev01;

n. EMC SourceOne for File Systems 7.2 Release Notes;

o. EMC SourceOne 7.2 Auditing and Reporting Installation and Administration Guide, Rev01; and

p. EMC SourceOne File Systems v7.2, Email Management v7.2, Discovery Manager v7.2, Offline Access v7.2, and for Microsoft SharePoint v7.1Guidance Documentation Supplement, Version 0.3.

9   Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of EMC SourceOne v7.2, including the following areas:

Development: The evaluators analyzed the EMC SourceOne v7.2 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the EMC SourceOne v7.2 security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the EMC SourceOne v7.2 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the EMC SourceOne v7.2 configuration management system and associated documentation was performed. The evaluators found that the EMC SourceOne v7.2 configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of EMC SourceOne v7.2 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the EMC SourceOne v7.2. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

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

10 ITS Product Testing

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

10.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[1].

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

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Auditing of Search Operations: The objective of this test goal is to verify that search operations are audited for SourceOne Search users;

c. Auditing of Search Functions by Active Directory Group: The objective of this test goal is to verify the search function permissions available to the Active Directory group and to confirm that the search functions are audited;

d. Auditing of Discovery Manager Operations: The objective of this test goal is to examine and confirm the auditing capabilities for the Discovery Manager; and

e. SourceOne Mapped Folder Access Control Policy: The objective of this test goal is to examine and confirm the SourceOne mapped folder access control policy for SourceOne Search.

10.3 Independent Penetration Testing

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

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities; and

---

[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.

b. Misuse Testing by TOE: The purpose of this test is to determine how the TOE responds to concurrent user logins.

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

10.4 Conduct of Testing

EMC SourceOne v7.2 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that EMC SourceOne v7.2 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

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

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 References

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

a.   CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b.   Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c.   Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d.   EMC SourceOne File Systems v7.2, Email Management v7.2, Discovery Manager v7.2, and for Microsoft SharePoint v7.1 Security Target, Version 1.6, January 6, 2015.

e.   Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of EMC SourceOne File Systems v7.2, Email Management v7.2, Discovery Manager v7.2, Offline Access v7.2, and for Microsoft SharePoint v7.1, Version 1.0, January 11, 2016.