



Certification Report

EAL 2+ Evaluation of EMC[®] VoyenceControl[™] v4.1.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment Canada, 2009

Document number: 383-4-110-CR
Version: 1.0
Date: 25 September 2009
Pagination: i to iv, 1 to 11



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 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. 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 Canada, 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 Canada, 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 Canada.

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 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 25 September 2009, 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 at: <http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html> and <http://www.commoncriteriaportal.org/>.

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

- EMC® is a registered trademark symbol of EMC Corporation;
- VoyenceControl™ is a trademark symbol of EMC Corporation;
- Microsoft, and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries;
- 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.; and
- Sun and Solaris are trademarks of Sun Microsystems, Inc. in the United States and other countries.

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

TABLE OF CONTENTS

Disclaimer i

Foreword ii

Executive Summary1

1 Identification of Target of Evaluation2

2 TOE Description2

3 Evaluated Security Functionality2

4 Security Target.....2

5 Common Criteria Conformance.....3

6 Security Policy.....3

7 Assumptions and Clarification of Scope3

 7.1 SECURE USAGE ASSUMPTIONS 3

 7.2 ENVIRONMENTAL ASSUMPTIONS 4

 7.3 CLARIFICATION OF SCOPE..... 4

8 Architectural Information4

9 Evaluated Configuration.....5

10 Documentation5

11 Evaluation Analysis Activities7

12 ITS Product Testing8

 12.1 ASSESSMENT OF DEVELOPER TESTS 8

 12.2 INDEPENDENT FUNCTIONAL TESTING..... 8

 12.3 INDEPENDENT PENETRATION TESTING 9

 12.4 CONDUCT OF TESTING 9

 12.5 TESTING RESULTS 9

13 Results of the Evaluation.....9

14 Evaluator Comments, Observations and Recommendations9

15 Acronyms, Abbreviations and Initializations.....10

16 References.....10

Executive Summary

EMC® VoyenceControl™ v4.1.0 (hereafter referred to as EMC VoyenceControl), from EMC Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

EMC VoyenceControl is an automated compliance management, change management, and configuration management solution. EMC VoyenceControl allows administrators to collaboratively manage their network infrastructure while enforcing control over change processes. End-users (both administrative and non-privileged) use EMC VoyenceControl as the central management “hub” for their Information Technology (IT) infrastructure – all changes to infrastructure devices are made via EMC VoyenceControl, which performs auditing of every change and pushes the changes out to the managed devices.

Electronic Warfare Associates-Canada, Ltd. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 31 August 2009 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 VoyenceControl, 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 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the EMC VoyenceControl 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 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 augmented evaluation is EMC® VoyenceControl™ v4.1.0 (hereafter referred to as EMC VoyenceControl), from EMC Corporation.

2 TOE Description

EMC VoyenceControl is an automated compliance management, change management, and configuration management solution. EMC VoyenceControl allows administrators to collaboratively manage their network infrastructure while enforcing control over change processes. End-users (both administrative and non-privileged) use EMC VoyenceControl as the central management “hub” for their IT infrastructure – all changes to infrastructure devices are made via EMC VoyenceControl, which performs auditing of every change and pushes the changes out to the managed devices.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for EMC VoyenceControl is identified in Section 6 (Security Requirements) and Section 7 (TOE Summary Specification) 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® VoyenceControl™ v4.1.0 Security Target, Evaluation Assurance Level: EAL2+

Version: 0.6

Date: 6 August 2009

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*.

EMC VoyenceControl version 4.1.0 is:

- a. *Common Criteria Part 2 conformant*, with security 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 augmented*, with all security the assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

EMC VoyenceControl enforces access and flow control security policies that control access to TOE functionality and resources. The policies are:

- A Management Access Control policy for TOE users and managed devices that controls their access to audit data and TOE configuration data;
- An Identification and Authentication (I&A) Access Control policy for TOE users and groups that controls their access to TOE user credentials and permissions; and
- A Device Information Flow Control policy for TOE users and managed devices that controls the flow of management data between TOE users and managed devices.

In addition, EMC VoyenceControl implements policies pertaining to security audit, identification and authentication, security management, protection of the TOE Security Functionality (TSF), and TOE access. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of EMC VoyenceControl should consider assumptions about usage and environmental settings as requirements for the product's installation and its operational 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:

- TOE users and administrators are non-hostile, appropriately trained, and follow all user guidance.

- Physical security will be provided for the TOE and its environment.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE operational environment must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
- The TOE operational environment will protect the TOE from external interference or tampering.
- The TOE operational environment will provide reliable timestamps for the TOE's use.

7.3 Clarification of Scope

The EMC VoyenceControl v4.1.0 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 VoyenceControl is a software-only network management tool. EMC VoyenceControl is designed to allow administrators to manage network devices from a central point on the network. Configuration changes for managed network devices are made on the EMC VoyenceControl and then pushed out to managed devices.

EMC VoyenceControl embodies a client-server architecture and consists of four (4) main components:

Application and Database Server. The Application and Database Server is the central network management “hub” of the product. It stores the data gathered and generated by the product which includes device configuration data and audit data;

Advisor Server. The Advisor Server hosts the report generators that analyze the device data stored by the product;

Device Server(s). The Device Server(s) communicates with the managed devices on the network on behalf of the Application Server; and

Management Client. The Management Client provides the primary administrative user interface for the product.

Each of these components is modular, and can be installed on a server by itself, or together with other components on the same server. EMC VoyenceControl is installed and deployed

on general-purpose server hardware running a general-purpose operating system as identified in the evaluated configuration.

9 Evaluated Configuration

The evaluated configuration for EMC VoyenceControl version 4.1.0.863 TOE comprises the following software components:

- Application Server Version 4.1.0.863;
- Device Server Release 12.0.863;
- Advisor Server Release 2.2.0.561 running the Report Advisor; and
- Thick Client.

EMC VoyenceControl was evaluated on the following operating systems (OS):

- Windows Server 2003 Enterprise Edition Service Pack 1;
- Red Hat Enterprise Linux 5 Server (update 3, x86_64);
- Red Hat Enterprise Linux 5 Advanced Platform (update 3, x86_64); and
- Solaris 10 Release 6/06

EMC VoyenceControl guidance on how to put the TOE in the evaluated configuration is:

- EMC Corporation VoyenceControl v4.1 Guidance Supplement, 0.1, 15 May 2009.

The guidance documentation is available online to registered customers from the EMC Powerlink site (<https://powerlink.emc.com>).

10 Documentation

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

- EMC VoyenceControl 4.1.0 Installing VoyenceControl on Solaris 10 P/N9 300-008-397 Rev A01;
- EMC VoyenceControl 4.1.0 Installing VoyenceControl on Red Hat Enterprise Linux 4 and 5 P/N 300-008-392 Rev A01;
- EMC VoyenceControl 4.1.0 Installing VoyenceControl on Windows Server 2003 P/N 300-008-395 Rev A01;

- EMC VoyenceControl 4.1.0 Release Notes P/N 300-008-381 Rev A01;
- EMC VoyenceControl 4.1.0 Cluster Installation Guide P/N 300-008-399 Rev A01;
- EMC VoyenceControl 4.1.0 GEO Diverse Installation Guide P/N 300-008-400 Rev A01;
- EMC VoyenceControl 4.1.0 Installing and Configuring the RSA Token Service on Windows Server 2003 P/N 300-008-636 Rev A01;
- EMC VoyenceControl 4.1.0 System Management Console Guide P/N 300-008-441 Rev A01;
- EMC VoyenceControl 4.1.0 Common Administration Guide for Integration Modules P/N 300-008-442 Rev A01;
- EMC VoyenceControl 4.1.0 Using Regular Expressions (RegEx) in VoyenceControl P/N 300-008-443 Rev A01;
- EMC VoyenceControl 4.1.0 Device Access Scripting Language (DASL) Specifications Guide P/N 300-008-444 Rev A01;
- EMC VoyenceControl 4.1.0 Backup and Recovery Guide P/N 300-008-445 Rev A01,
- EMC VoyenceControl Application Program Interface (API) 4.1.0 Programmer's Guide P/N 300-008-447 Rev A01;
- EMC VoyenceControl 4.1.0 Troubleshooting Guide P/N 300-008-449 Rev A01;
- EMC VoyenceControl 4.1.0 Online User's Guide P/N 300-008-449 Rev A01; and
- Various migration guides and integration modules documentation.

11 Evaluation Analysis Activities The evaluation analysis activities involved a structured evaluation of EMC VoyenceControl, including the following areas:

Development: The evaluators analyzed the EMC VoyenceControl functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces (TSFI), the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the EMC VoyenceControl security architectural description and determined that the initialization process was 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 were correct.

Guidance Documents: The evaluators examined the EMC VoyenceControl preparative procedures and operational user guidance and determined that it sufficiently and unambiguously described 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 procedures and operational user guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the EMC VoyenceControl configuration management system and associated documentation was performed. The evaluators found that the EMC VoyenceControl configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

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

The evaluators reviewed the flaw remediation procedures used by EMC Corporation for EMC VoyenceControl. 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.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of EMC VoyenceControl. Additionally, the evaluators conducted a independent review of public domain vulnerability databases and all evaluation deliverables to identify EMC VoyenceControl potential vulnerabilities. The evaluators penetration testing did not expose any vulnerabilities that would be exploitable in the intended operational environment.

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 penetration tests.

12.1 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 ETR².

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.

12.2 Independent Functional Testing

During this evaluation, the evaluators developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, 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. Resulting from this test coverage approach was the following list of Electronic Warfare Associates-Canada test goals:

- **Initialization:** The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance.
- **Repeat of Developer's Tests:** The objective of this test goal is to repeat a subset of the developer's tests to gain confidence in the developer's testing process and results.
- **TOE Access:** The objective of this test goal is to verify the user access security features of the TOE.
- **Identification and Authentication:** The objective of this test goal is to verify the TOE security functionality requires users be successfully identified and authenticated.
- **Security Management:** The objective of this test is to verify the TOE's management of user and group permissions.

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.

- User Data Protection: The objective of this test is to verify the flow of configuration data from the TOE to a managed device.

12.3 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:

- Generic vulnerabilities;
 - The objective of this test is to check the robustness of the product in dealing with unexpected events.
 - The objective of this test is to verify the server on which the TOE operates has the expected ports open and the expected services available.

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

12.4 Conduct of Testing

EMC VoyenceControl was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Testing (ITSET) Facility at Electronic Warfare Associates-Canada. 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 a separate Test Results document.

12.5 Testing Results

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

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 EMC VoyenceControl documentation set includes comprehensive installation, administration, deployment, development, user, and reference guides. The developer also provides a complete solution with on-site system engineer to help the customer integrate the TOE into a corporate network. 24/7 support is also an available option.

EMC Support was used by the evaluator to report a documentation issue and found to provide a timely response and solution.

15 Acronyms, Abbreviations and Initializations

<u>Acronym/Abbreviation/ Initialization</u>	<u>Description</u>
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
I&A	Identification and Authentication
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
JRE	Java Runtime Environment
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
QA	Quality Assurance
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF interfaces

16 References

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

- a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.
- b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.
- c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.
- d. EMC Corporation EMC® VoyenceControl™ v4.1.0 Security Target, Evaluation Assurance Level: EAL2+, Version 0.6, 6 August 2009

- e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of EMC Corporation EMC® VoyenceControl™ v4.1.0, Document No. 1614-000-D002, Version 1.3, 31 August 2009