Certification Report

EAL 2+ Evaluation of EMC® Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-187-CR
Version: 1.0
Date: 12 April 2012
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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 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 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 EWA-Canada located in Ottawa, 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, 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 12 April 2012, 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 trademarks or registered trademarks:

- SMARTS is a registered trademark symbol of EMC Corporation.
- EMC is a registered trademark symbol of EMC Corporation.
- Ionix is a trademark of EMC Corporation.

TABLE OF CONTENTS

Executive Summary

EMC® Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3 (hereafter referred to as EMC Ionix), from EMC Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

EMC Ionix is a collection of software products which monitor IT networks. EMC Ionix can map networks, monitor the availability and performance of network nodes, and show the business implications of any failures. EMC Ionix 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 network problem.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 28 March 2012 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 Ionix, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the EMC Ionix 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® Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3 (hereafter referred to as EMC Ionix, from EMC Corporation.

2 TOE Description

EMC Ionix is a collection of software products which monitor IT networks. EMC Ionix can map networks, monitor the availability and performance of network nodes, and show the business implications of any failures. EMC Ionix 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 network problem. The following provides a brief description of the TOE components:

- Service Assurance Manager (SAM) - The core management server for the whole system.
- SAM Adapters - Provides modular communication with and monitoring of other components
- Global Console - The primary management interface to the Service Assurance Manager. Business Impact Manager - Extends the capabilities of the SAM by calculating the business impact of events.
- Business Dashboard - Extends the capabilities of the SAM by presenting the business impacts of events.
- Report Manager - Extends the capabilities of the SAM by storing events in a database ready to be compiled into reports.
- Broker - Manages a registry of EMC Ionix server applications.
- IP Availability Manager - Monitors the availability of IP networks
- IP Performance Manager - Monitors the performance of IP networks.
- IP Server Performance Manager - Monitors the performance of critical servers.
- EMC Ionix Server Manager (EISM) - Monitors the availability of virtual servers and clusters.
- Storage Insight for Availability (SIA) - Provides Storage Area Network and Network Attached Storage monitoring services.
- Network Protocol Manager (NPM) -Monitors layer 3 routing devices.

A detailed description of the EMC Ionix architecture is found in Section 1.5 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for EMC Ionix is identified in Section 6 of the ST.

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: EMC Corporation® Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3 Security Target
Version: 0.8
Date: 17 February 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

EMC Ionix is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - EXT_INX_MDC.1 - Monitored Resource Data Collection;
   - EXT_INX_RCA.1 - Root Cause Analysis;
   - EXT_INX_ARP.1 - Resource Availability Alarms; and
   - EXT_INX_RDR.1 - Restricted Data Review.

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*, containing all security assurance requirements in the EAL 2 package, as well as the following: e.g. ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

EMC Ionix implements a role-based access control policy to control administrator access to the system. Details of this security policy can be found in Section 6 of the ST.

In addition, EMC Ionix implements policies pertaining to security audit, identification and authentication, security management, TOE access and IT operations intelligence. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of EMC Ionix 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 are one or more competent individuals assigned to manage the TOE; and
- The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

7.2 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 monitor its resources;
- 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; and
- The communication between the TOE and its monitored resources will be protected from alteration or impersonation.

7.3 Clarification of Scope

EMC Ionix offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. EMC Ionix is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for EMC Ionix comprises the following software components:

- SAM version 8.1.1.0 build 19;

- Global Console version 8.1.1.0 build 990;
- Business Impact Manager version 8.1.1.0 build 19;
- Business Dashboard version 8.1.1.0 build 19;
- Broker version 8.1.1.0 build 19;
- Report Manager version 1.3.0.0 build 28;
- IP Availability Manager version 8.1.1.0 build 59;
- IP Performance Manager version 8.1.1.0 build 59;
- IP Sever Performance Manager version 8.1.1.0 build 59;
- NPM version 3.1.2.0 build 4;
- SIA version 2.3.1.1 build 2;
- EISM version 3.0.0.0 build 91; and
- SAM Adapter version 1.3.0.0 build 28.

Table 3 of the ST specifies tested platforms and architectures for the TOE components in the CC-evaluated configuration.

The publication entitled *EMC Corporation Ionix Suite for IT Operations Intelligence (SMARTS) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3 Guidance Documentation Supplement* describes the procedures necessary to install and operate EMC Ionix in its evaluated configuration.

9 Documentation

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

- EMC Ionix Service Assurance Management Suite Deployment Guide, April 2011;
- EMC Ionix Service Assurance Management Suite Installation and Migration Guide, April 2011;
- EMC Ionix Service Assurance Manager Operator Guide, June 2011;
- EMC Ionix Service Assurance Manager Configuration Guide, April 2011;
- EMC Ionix Service Assurance Manager Dashboard Configuration Guide, April 2011;
- EMC Ionix Business Impact Manager User Guide, April 2011;
- EMC Ionix Service Assurance Manager Failover System User Guide, April 2011;
- EMC Ionix Service Assurance Manager Adapter Platform User Guide, April 2011;
- EMC Ionix Service Assurance Manager Notification Adapters User Guide, April 2011;
- EMC Ionix XML Adapter User Guide, April 2011;
- EMC Ionix Storage Insight for Availability Discovery Guide, October 2010;
- EMC Ionix Storage Insight for Availability Installation and Configuration Guide, October 2010;
- EMC Ionix Storage Insight for Availability User Guide, October 2010;
- EMC Ionix IP Management Suite Installation Guide, March 2011;
- EMC Ionix IP Management Suite Deployment Guide, March 2011;
- EMC Ionix IP Management Suite Configuration Guide, March 2011;

- EMC Ionix IP Management Suite Discovery Guide, March 2011;
- EMC Ionix IP Availability Manager User Guide, March 2011;
- EMC Ionix IP Performance Manager and Server Performance Manager User Guide, November 2010;
- EMC Ionix IP Availability Manager Extension for NAS User Guide, May 2011;
- EMC Ionix Server Manager Installation Guide, April 2011;
- EMC Ionix Server Manager Configuration Guide, April 2011;
- EMC Ionix Server Manager User Guide, April 2011;
- EMC Ionix Network Protocol Management Suite Installation Guide, December 2010;
- EMC Ionix Network Protocol Manager for BGP User's Guide, December 2010;
- EMC Ionix Network Protocol Manager for EIGFP User's Guide, December 2010;
- EMC Ionix Network Protocol Manager for IS-IS User's Guide, December 2010;
- EMC Ionix Network Protocol Manager for OSPF User's Guide, December 2010;
- EMC Ionix Network Protocol Manager Configuration Guide, December 2010;
- EMC Ionix Network Protocol Manager Discovery Guide, December 2010;
- EMC Ionix Adapter for Concord eHealth User Guide, November 2010;
- EMC Ionix Adapter for InfoVista User Guide, November 2010;
- EMC Ionix Adapter for Microsoft Operations Manager 2005 User Guide, November 2010;
- EMC Ionix Adapter for Microsoft System Center Operations Manager 2007 User Guide, November 2010;
- EMC Ionix Adapter for NetIQ AppManager User Guide, November 2010;
- EMC Ionix Adapter for Remedy ARS User Guide, November 2010;
- EMC Ionix Adapter for SiteScope User Guide, November 2010;
- EMC Ionix SQL Data Interface Adapter User Guide, November 2010;
- EMC Ionix Report Manager User Guide, November 2010;
- EMC Ionix Service Assurance Manager Adapters Suite and Report Manager Installation Guide, November 2010;
- EMC Ionix Foundation 9.0 ITOps[2] System Administration Guide, December 2010; and
- EMC Corporation Ionix Suite for IT Operations Intelligence (SMARTS) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3 Guidance Documentation Supplement v0.1, August 2011

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of EMC Ionix, including the following areas:

[2] IT Operations

Development: The evaluators analyzed the EMC Ionix 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 Ionix 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 Ionix 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 Ionix configuration management system and associated documentation was performed. The evaluators found that the EMC Ionix 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 Ionix during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by EMC Corporation for EMC Ionix. 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 Ionix. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify EMC Ionix potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to EMC Ionix in its operational environment.

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

11 ITS Product Testing

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

11.1 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[3].

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.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, 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 is the following list of EWA-Canada 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. Security Management – User Administration: The purpose of this test case is to verify that the administrator with 'All' role has access to sufficient security management functionality to create and customize permissions for console users; and

c. SAM Adapters - Remedy Adapter: The purpose of this test case is to test the Adapter Command Line Interface (CLI) by exercising the link from the SAM Remedy Adapter to a Remedy server.

11.3 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. Misuse Testing: The purpose of this test case is to verify that the TOE will continue to operate as expected when a component returns to operation after becoming unavailable due to administrator error; and

[3] 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. Monitor for Information Leak: The purpose of this test case is to verify that the TOE does not leak sensitive information during login.

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

11.4 Conduct of Testing

EMC Ionix was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the developer's testing facility located in White Plains, New York. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

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

12 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.

13 Evaluator Comments, Observations and Recommendations

The complete documentation set for EMC Ionix provides a mature, comprehensive set of instructions for planning, installation and use.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
EISM	EMC Ionix Server Manager
ETR	Evaluation Technical Report
IP	Internet Protocol
IT	Information Technology

Acronym/Abbreviation/ Initialization	Description
ITOps	IT Operations
ITSET	Information Technology Security Evaluation and Testing
NPM	Network Protocol Manager
PALCAN	Program for the Accreditation of Laboratories - Canada
SAM	Service Assurance Manager
SFR	Security Functional Requirement
SIA	Storage Insight for Availability
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 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 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. EMC Corporation® Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3 Security Target, 0.8, 17 February 2012.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of EMC Corporation Ionix™ for IT Operations Intelligence (SMARTS®) - SAM 8.1.1, IP 8.1.1, NPM 3.1, SIA 2.3.1.1, EISM 3.0, SAM Adapters 1.3 Document No. 1694-000-D002, Version 1.3, 28 March 2012.