Certification Report

EAL 3+ Evaluation of Novell Identity Manager 4.0.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-214-CR
Version: 1.0
Date: 26 March 2013
Pagination: i to iii, 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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.

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 26 March 2013, 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).

TABLE OF CONTENTS

Executive Summary

Novell Identity Manager 4.0.2 (hereafter referred to as IDM 4.0.2), from NetIQ Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

IDM 4.0.2 is a data sharing and synchronization service that enables applications, directories, and databases to share information. It links scattered information and enables policies that govern automatic updates to designated systems when identity changes occur. IDM 4.0.2 provides the foundation for account provisioning, security, single sign-on, user self-service, authentication, authorization, automated workflow, and Web services. It allows administrators to integrate, manage, and control distributed identity information in a secure manner.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 6 March 2013 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 IDM 4.0.2, 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 3 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.* The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the IDM 4.0.2 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] 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) 3 augmented evaluation is Novell Identity Manager 4.0.2 (hereafter referred to as IDM 4.0.2), from NetIQ Corporation.

2 TOE Description

IDM 4.0.2 is a data sharing and synchronization service that enables applications, directories, and databases to share information. It links scattered information and enables policies that govern automatic updates to designated systems when identity changes occur. IDM 4.0.2 provides the foundation for account provisioning, security, single sign-on, user self-service, authentication, authorization, automated workflow, and Web services. It allows administrators to integrate, manage, and control distributed identity information in a secure manner.

A detailed description of the IDM 4.0.2 architecture is found in Section 1.7 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for IDM 4.0.2 is identified in Section 7 of the ST.

4 Security Target

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

Title: Security Target: Novell Identity Manager 4.0.2
Version: 1.3
Date: 29 January 2013

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.*

IDM 4.0.2 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 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation

6 Security Policy

IDM 4.0.2 implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section 7.3 of the ST.

In addition, IDM 4.0.2 implements insert other policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of IDM 4.0.2 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Administrators of the TOE are appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.

- Administrators of the TOE and users on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The processing platforms on which the TOE resides are located within a facility that provides controlled access.
- The TOE is configured to receive all passwords and associated data from network‐attached systems.
- The TOE has a trusted source for system time via NTP server.

7.3 Clarification of Scope

IDM 4.0.2 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. IDM 4.0.2 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The TOE consists of a set of software applications run on one or multiple distributed systems; it can also run on a virtual machine. The TOE requires the following software components:

Component	Requirements
Administration Workstation	Web Browsers • Internet Explorer 7, 8, and 9. • Mozilia Firefox 3, 3.5, 3.6, 4 Designer & Analyzer • SLES 10 SP3 (32 and 64-bit) • SLES 11 (32 and 64-bit) • SLES 11 SPI (32 and 64-bit) • Windows 7 (32 and 64-bit) • Windows Server 2003 SP2 (32-bit only)

	• Windows Server 2008 R2: (64-bit only) • Solaris 10 (64-bi t) • Windows Server 2008 SPI or later (32 or 64 bit)
User Application Server 4.0.2 / Reporting Server	• SLES 10 SP3 (32: and 64-bit) • SLES 11 (32: and 64-bit) • SLES 11 SPI (32: and 64-bit) • OES 2: SP3 (32: and 64-bit) • RHEL 5.4 (32: and 64-bit) • RHEL 6.0 (32: and 64-bit) • Windows Server 2003 SP2: (3 2: -bit only) • Windows Server 2008 R2: (64-bit only) • Windows Server 2008 SPI (32 and 64-bit only)
Meta-directory 4.0.2. Server (Identity Vault, Meta-directory Engine, and Remote loader)	• iManager 2.7.5 • SLES 10 SP3 (32 and 64-bit) • SLES 11 (32 and 64-bit) • SLES 11 SP1 (32 and 64-bit) • RHEL 5.4 (32 and 64-bit) • RHEL 6.0 (32 and 64-bit) • Windows Server 2003 SP2 (32-bit only) • Windows Server 2008 R2 (64-bit only)
Role Mapping Administrator Web Services	• iManager 2.7.5 • SLES 10 SP3 (32 and 64-bit)

	• SLES 11 (32 and 64-bit) • SLES 11 SPI (32 and 64-bit) • RHEL 5.4 (32 and 64-bit) • RHEL 6.0 (32 and 64-bit) • Windows Server 2003 SP2 (32-bit only) • Windows Server 2008 R2 (64-bit only)
Event Auditing Service	• SLES 10 SP3 (32 and 64-bit) • SLES 11 (32 and 64-bit) • SLES 11 SPI (32 and 64-bit)
Virtual Machine Support	• Xen v4.2 • Windows Server 2008 R2 Virtualization with Hyper-V • VMware ESX 4.0,ESXi 4.0,4.1, ESXi 5.0 • VMware Workstation 6.5.

The publication entitled Operational User Guidance and Preparative Procedures Supplement Novell Identity Manager 4.0 describes the procedures necessary to install and operate IDM 4.0.2 in its evaluated configuration.

9 Documentation

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

a. User Application: Administration Guide Novell identity Manager Roles Based Provisioning Module 4.0;

b. Understanding Policies: Novell Identity Manager 4.0;

c. Identity Reporting Module Guide: Novell Identity Manager 4.0.2;

d. Overview Guide Novell Identity Manager 4.0;

e. Installation Guide: Novell Identity Manager 4.0.2;

f. User Application: Installation Guide: Novell Identity Manager Roles Based Provisioning Module 4.0.2;

g. Integrated Installation Guide: Novell Identity Manager 4.0;

h. Role Mapping Administrator Installation and Configuration Guide: Identity Manager 4.0.2; and

i. Installation Guide: eDirectory 8.8 SP7

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of IDM 4.0.2, including the following areas:

Development: The evaluators analyzed the IDM 4.0.2 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 IDM 4.0.2 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 IDM 4.0.2 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 IDM 4.0.2 configuration management system and associated documentation was performed. The evaluators found that the IDM 4.0.2 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 IDM 4.0.2 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for IDM 4.0.2 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.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of IDM 4.0.2. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify IDM 4.0.2 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to IDM 4.0.2 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 3 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[2].

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. User account management: The objectives of this test goal is to confirm that the TOE can create and modify the privilege level of user accounts, and that only administrators can modify/delete security attributes of users ;

[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.

c. Event Analysis report generation: The objective of this test goal is to confirm that the TOE can generate reports based upon audit entries for security activities; and

d. Access Control: The objective of this test goal is to confirm that the TOE implements and enforces an access control policy for use of TOE functions.

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. Port Scan: The objective of this test goal is to scan the TOE using a port scanner to identify open ports for potential issues;

b. Vulnerability Identification: Tool Scanning: The objective of this test goal is to scan the TOE for vulnerabilities using automated tools; and

c. Information Leakage Verification: The objective of this test goal is to monitor the TOE for leakage during start-up, shutdown, login, and other scenarios using a packet sniffer.

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

11.4 Conduct of Testing

IDM 4.0.2 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 Test (ITSET) Facility at EWA-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.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that IDM 4.0.2 behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 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
RHEL	Red Hat Enterprise Linux
SLES	SUSE Linux Enterprise Server
ST	Security Target
TOE	Target of Evaluation

14 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. Security Target: Novell Identity Manager 4.0.2, 1.3, 29 January 2013 .

e. Evaluation technical Report for EAL 3+ Common Criteria Evaluation of Novell Identity Manager 4.0.2, v1.1, 6 March 2013.