Certification Report

Centrify Suite version 2013.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-238-CR
Version:	1.0
Date:	23 October 2013
Pagination:	i to iii, 1 to 8

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 23 October 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).

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

- Linux is a registered trademark of Linus Torvalds Inc.
- Macintosh is a registered trademark of Apple, Inc.
- Windows is a registered trademark of Microsoft Corporation.

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

TABLE OF CONTENTS

Executive Summary

Centrify Suite version 2013.2 (hereafter referred to as Centrify Suite), from Centrify Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Centrify Suite provides Active Directory-based authentication, access control, identity management and group policy support for Unix based platforms such as Linux and Macintosh. Through the DirectManage Access Manager component, Active Directory users and groups may be assigned UNIX identity attributes such that role-based access control (RBAC) rights and roles may be applied on these non-Windows servers and workstations. The UNIX components implement the authentication and identity mapping functions necessary for Active Directory users and groups to behave like UNIX users and groups on UNIX platforms.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 18 September 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 Centrify Suite, 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.* The following augmentation is claimed: e.g. ALC_FLR.1 – Basic Flaw Remediation

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Centrify 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) 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 Centrify Suite version 2013.2 (hereafter referred to as Centrify Suite), from Centrify Corporation.

2 TOE Description

Centrify Suite provides Active Directory-based authentication, access control, identity management and group policy support for Unix based platforms such as Linux and Macintosh. Through the DirectManage Access Manager component, Active Directory users and groups may be assigned UNIX identity attributes such that role-based access control (RBAC) rights and roles may be applied on these non-Windows servers and workstations.   The UNIX components implement the authentication and identity mapping functions necessary for Active Directory users and groups to behave like UNIX users and groups on UNIX platforms.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Centrify Suite is identified in Section 6 of the Security Target (ST).

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
Centrify Cryptographic Module	1604

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Centrify Suite:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	1018, 1208
Advanced Encryptions Standard (AES)	FIPS 197	1554, 1861
Secure Hash Standard (SHS)	FIPS 180-3	1375, 1637
Deterministic Random Bit Generators (DRBG)	FIPS 197	69, 149
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	904, 1108

4 Security Target

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

Title: Security Target for Centrify Suite version 2013.2
Version: 0.89
Date: 12 September 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.*

Centrify Suite is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST:

   • FTA_IDM_EXT.1 – Identity Management.

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.1 – Basic Flaw Remediation

6 Security Policy

Centrify Suite implements policies pertaining to security audit, cryptographic support, identification and authentication, TOE access, Trusted path/channels and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Centrify Suite 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 competent individuals assigned to manage the TOE and the security of the information it contains;
- The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation; and
- The TOE can only be accessed by authorized users.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access; and
- The TOE is installed on the appropriate, dedicated hardware and operating system.

8 Evaluated Configuration

The evaluated configuration for Centrify Suite comprises:

- Centrify DirectControl UNIX Agent (Redhat) version 5.1.1 build 831 on RHEL5;
- Centrify DirectControl UNIX Agent (Mac) version 5.1.1 build 831 on Mac10.6 and Mac 10.7;
- DirectManage Access Manager version 5.1.1 build 831 on Windows 7; and
- DirectManage ADUC (Active Directory Users and Computers) Snap-in 5.1.1 build 831 on Windows 2008.

The publication entitled Centrify Suite 2013 Operational User Guidance and Preparative Procedures Supplement for Common Criteria, document version 1.2, September 2013 describes the procedures necessary to install and operate Centrify Suite in its evaluated configuration.

9 Documentation

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

- Centrify Suite 2013 Operational User Guidance and Preparative Procedures Supplement for Common Criteria, document version 1.2, September 2013;
- Centrify Suite 2013 Administrator’s Guide for Linux and UNIX, June 2013;
- Centrify Suite 2013 Configuration and Tuning Reference Guide, June 2013;
- Centrify Suite 2013 Planning and Deployment Guide, June 2013;
- Centrify Suite 2013 Administrator’s Guide For Mac OS X, June 2013; and
- Centrify Suite 2013 Group Policy Guide, June 2013.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Centrify Suite, including the following areas:

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

The evaluators reviewed the flaw remediation procedures used by developer for the Centrify Suite. 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 Centrify Suite. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Centrify Suite potential vulnerabilities. The evaluators identified potential vulnerabilities; subsequent to follow-on penetration testing (ref: section 11.3) it was verified that none of the potential vulnerabilities were exploitable in the operational environment for Centrify Suite.

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

11 ITS Product Testing

Testing 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. Initialization: The objective of this test goal is to show that the TOE can be installed and configured into its evaluated configuration;

c. Identity Management (Redhat and Mac): The objective of this test goal is to show that the TOE provides the security functions required to establish a session on a UNIX resource;

d. Authentication failure Handling (Redhat and Mac): The objective of this test goal is to confirm that the TOE enforces offline authentication failure handling on both Redhat and Mac; and

e. Inter-TSF Trusted channel: The objective of this test goal is to demonstrate that the TOE provides a secure channel for the purpose of either reading or writing Active Directory security objects and attributes.

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:

[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.

a. Port Scan: The objective of this test goal is to confirm that only the expected ports were found open on the Windows, Redhat Linux, and Mac operating system;

b. Tool Scanning: The objective of this test goal is to scan for known and unknown weaknesses relevant to the TOE type; and

c. Escalation of privilege vulnerabilities: The objective of this test goal is for a user to attempt to escalate their privileges on the TOE.

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

11.4 Conduct of Testing

Centrify Suite 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 Centrify Suite 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

Centrify Suite 2013.2 includes a mature, comprehensive set of user documents. Implementers of the TOE should pay particular attention to the configuration instructions in the Guidance Supplement in order to ensure the proper implementation of the evaluated configuration.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
3DES	Triple-DES
ADUC	Active Directory Users and Computers
AES	Advanced Encryption Standard
CCEF	Common Criteria Evaluation Facility

Acronym/Abbreviation/ Initialization	Description
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DRBG	Deterministic Random Bit Generators
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMAC	Keyed-Hash Message Authentication Code
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
RBAC	Role-Based Access Control
RHEL	Red Hat Enterprise Linux
SHS	Secure Hash Standard
SFR	Security Functional Requirement
ST	Security Target
TSF	TOE Security Functionality
TOE	Target of Evaluation

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 4, September 2012.

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

d. Security Target for Centrify Suite version 2013.2, 0.89, 12 September 2013.

e. ETR for Centrify Corporation Centrify Suite Version 2013.2, v1.1, 18 September 2013.