



Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR **CYBER SECURITY**

COMMON CRITERIA CERTIFICATION REPORT

Dell EMC™ SupportAssist Enterprise 4.0

with Policy Manager 6.8

Dell EMC

6 August 2020

487 EWA 2019



FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

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 Centre for Cyber Security (CCCS). 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 Canadian CC Scheme, 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 Canadian Centre for Cyber Security, 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 Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Contact Centre and Information Services

Edward Drake Building

contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)



OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the 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.

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



TABLE OF CONTENTS

EXECUTIVE SUMMARY	6
1 Identification of Target of Evaluation	7
1.1 Common Criteria Conformance	7
1.2 TOE Description.....	7
1.3 TOE Architecture	8
2 Security Policy.....	9
2.1 Cryptographic Functionality	9
3 Assumptions and Clarification of Scope	10
3.1 Usage and Environmental Assumptions.....	10
3.2 Clarification of Scope	10
4 Evaluated Configuration.....	11
4.1 Documentation.....	11
5 Evaluation Analysis Activities	12
5.1 Development.....	12
5.2 Guidance Documents.....	12
5.3 Life-Cycle Support	12
6 Testing Activities	13
6.1 Assessment of Developer tests.....	13
6.2 Conduct of Testing	13
6.3 Independent Functional Testing	13
6.3.1 Functional Test Results.....	13
6.4 Independent Penetration Testing.....	14
6.4.1 Penetration Test results.....	14
7 Results of the Evaluation	15
7.1 Recommendations/Comments.....	15
8 Supporting Content.....	16
8.1 List of Abbreviations.....	16



8.2 References.....16

LIST OF FIGURES

Figure 1: TOE Architecture..... 8

LIST OF TABLES

Table 1: TOE Identification 7

Table 2: Cryptographic Implementation(s)..... 9



EXECUTIVE SUMMARY

The Dell EMC™ SupportAssist Enterprise 4.0 with Policy Manager 6.8 (hereafter referred to as the Target of Evaluation, or TOE), from Dell EMC, was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 6 August 2020 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for TOE, 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.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian CC Scheme and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Dell EMC™ SupportAssist Enterprise 4.0 with Policy Manager 6.8
Developer	Dell EMC

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

EAL 2+ (ALC_FLR.2)

1.2 TOE DESCRIPTION

The TOE is an asynchronous messaging system in which all communications are initiated from the customer site. All communications between the customer's SAE implementation and the Dell EMC Enterprise servers use the Hypertext Transfer Protocol Secure (HTTPS) protocol with end-to-end Transport Layer Security (TLS) tunneling.

The TOE is used by Dell EMC hardware and software at customer sites to send a variety of information including configuration data, logs, error messages, usage and performance data to Dell EMC and to allow identified Dell EMC support personnel remote access to those systems for troubleshooting.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

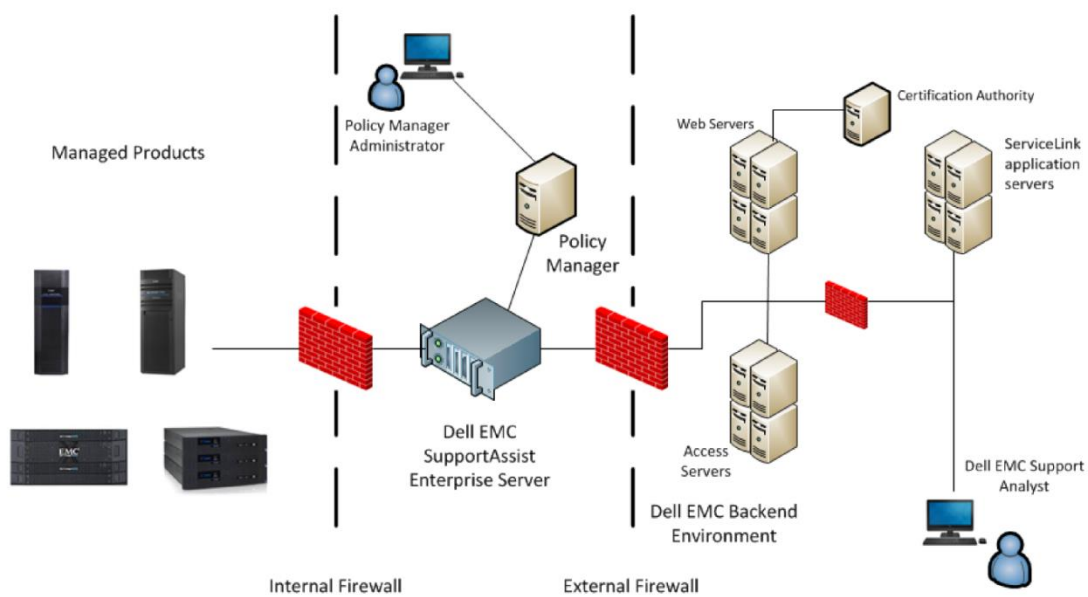


Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementation has been evaluated by the CMVP and is used by the TOE:

Table 2: Cryptographic Implementation

Cryptographic Module	Certificate Number
OpenSSL FIPS Object Module (2.0.2)	#1747

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE is connected to the network in such a way that it is able to access all of the access-controlled resources.
- The operational environment will be responsible for protecting the communications link between the Policy Manager and the SupportAssist Enterprise Server and between the Policy Manager and administrative users.
- The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.2 CLARIFICATION OF SCOPE

The following features are excluded from this evaluation:

- Remote user authentication verified through Dell EMC network security
- Automatic software updates

Additionally, it should be noted that security provided by the managed product is not part of the evaluated functionality. If a connection from the Dell EMC infrastructure to the managed product is allowed, the connection then relies on the security functionality provided by the managed product itself. If authentication is enforced by the managed product, then Dell EMC support personnel must be provided with the appropriate credentials for logging in.

Implementers must ensure that if multiple managed products are available on the same subnet, that all these products are appropriately configured to control access. Otherwise, a support representative granted access to troubleshoot one device, may inadvertently have access to other devices on that subnet as well.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

The TOE software (SAE VE 4.00.00.08 and Policy Manager 6.8.3 Build 129692) running on:

- A server running VMware ESXi 6.7 (Virtualized SAE running on SLES 12 SP3)
- A server running Windows Server 2012 R2 (Policy Manager 6.8)

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

- a) SupportAssist Enterprise Version 4.0 Technical Description Guide, July 2019
- b) Secure Remote Services Policy Manager, Version 6.8, Operations Guide, 2018
- c) Dell EMC™ SupportAssist Enterprise 4.0 Common Criteria Guidance Supplement, Version 1.3
- d) SupportAssist Enterprise Version 4.0 User's Guide, July 2019
- e) SupportAssist Enterprise Version 4.0 Troubleshooting Guide, July 2019
- f) SupportAssist Enterprise Version 4.0 Reportable Items, July 2019
- g) SupportAssist Enterprise Version 4.0 Alert Policy Guide, July 2019
- h) SupportAssist Enterprise Version 4.0 Support Matrix, July 2019
- i) Secure Remote Services Policy Manager, Version 6.8, Policy Manager
- j) Installation Guide using Locally-Installed Directory Service (OpenDS), November 2018

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

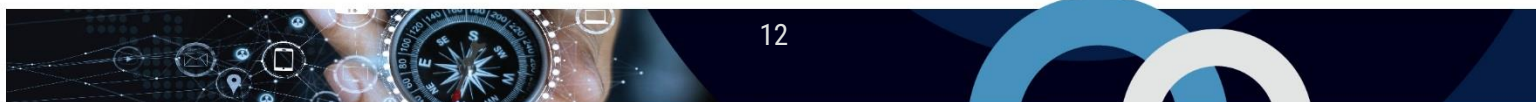
The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the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

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE 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 the TOE during distribution to the consumer.



6 TESTING ACTIVITIES

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

6.1 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 Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE 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.

6.3 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. The following testing activities were performed:

- a. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests
- b. Verification of the Cryptographic Implementation: The evaluator verified that the claim implementation was present and used by the TOE
- c. Concurrent Management Sessions: The evaluator verified that multiple concurrent management sessions can be accommodated
- d. Inter-TSF Confidentiality: The evaluator verified that communication between the TOE and Dell EMC is protected

6.3.1 FUNCTIONAL TEST RESULTS

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

6.4 INDEPENDENT PENETRATION TESTING

The penetration testing effort focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their penetration testing effort.

6.4.1 PENETRATION TEST RESULTS

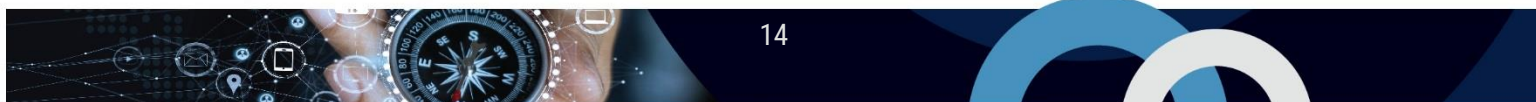
Type 1 & 2 searches were conducted on 3/11/2020 and included the following search terms:

- SupportAssist Enterprise 4.0
- Policy Manager 6.8
- Policy Manager 6.8.3

Vulnerability searches were conducted using the following sources:

- National Vulnerability Database: <https://nvd.nist.gov/vuln/search>
- EMC support: <https://support.emc.com/>
- Common Vulnerabilities and Exposures: <http://google.ca>

CVE-2018-15764 and CVE-2017-4976 were found for Policy Manager 6.8. Users are instructed to follow the guidance provided by the vendor to mitigate these vulnerabilities.



7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

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 Centre for Cyber Security (CCCS). This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.



8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CCCS	Canadian Centre for Cyber Security
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Security Target Dell EMC™ SupportAssist Enterprise 4.0 with Policy Manager 6.8, 9 April 2020, v1.2
Evaluation Technical Report Dell EMC™ SupportAssist Enterprise 4.0 with Policy Manager 6.8, 6 August 2020, v1.0