



Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR **CYBER SECURITY**

COMMON CRITERIA CERTIFICATION REPORT

Dell EMC Unity OE v5.2

13 December 2022

578-LSS

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 testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). 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 Common Criteria Program, and the conclusions of the testing laboratory 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 organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security

Contact Centre and Information Services

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



OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL 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, 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 CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).



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
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 Testing.....	13
6.3.1 Independent Testing Results	13
6.4 Vulnerability Analysis	14
6.4.1 Vulnerability Analysis 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



EXECUTIVE SUMMARY

Dell EMC Unity OE v5.2 (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.

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on **13 December 2022** and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the 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 Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

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 Unity OE v5.2
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:

EAL2+ with ALC_FLR.2

1.2 TOE DESCRIPTION

The TOE is a storage array system comprised of the Unity hardware platform and the Unity Operating Environment software.

The Unity hardware houses the disks in the storage array which are managed by the storage processors. It provides Network Access Server (NAS) and Storage Area Network (SAN) services by interfacing with the front-end clients (application hosts) and the back-end storage disks.

Application hosts can access the Unity storage through traditional block and file protocols. The TOE presents storage to application hosts as a standard network-based virtual file server, or in the form of Logical Units (LUNs) to block-based client machines.

The TOE supports the following storage protocols:

- File Storage Protocols
 - Common Internet File System (CIFS) / Server Message Block (SMB v2 and v3)
 - Network File System (NFS v3, v4, and v4.1)
- Block Storage Protocols
 - Internet Small Computer System Interface (iSCSI)
 - Fibre Channel (FC)

The TOE is managed by authorized administrators through the Unified Element Management Command Line Interface (UEMCLI), the Unisphere Graphical User Interface (GUI) and the Representational State Transfer Application Programming Interface (REST API). Administrators are assigned a user role that provides them with access to specific TOE features and functions.

1.3 TOE ARCHITECTURE

The TOE is a stand-alone appliance consisting of the Unity hardware platform and the Unity Operating Environment software.

A diagram of the TOE architecture is as follows:

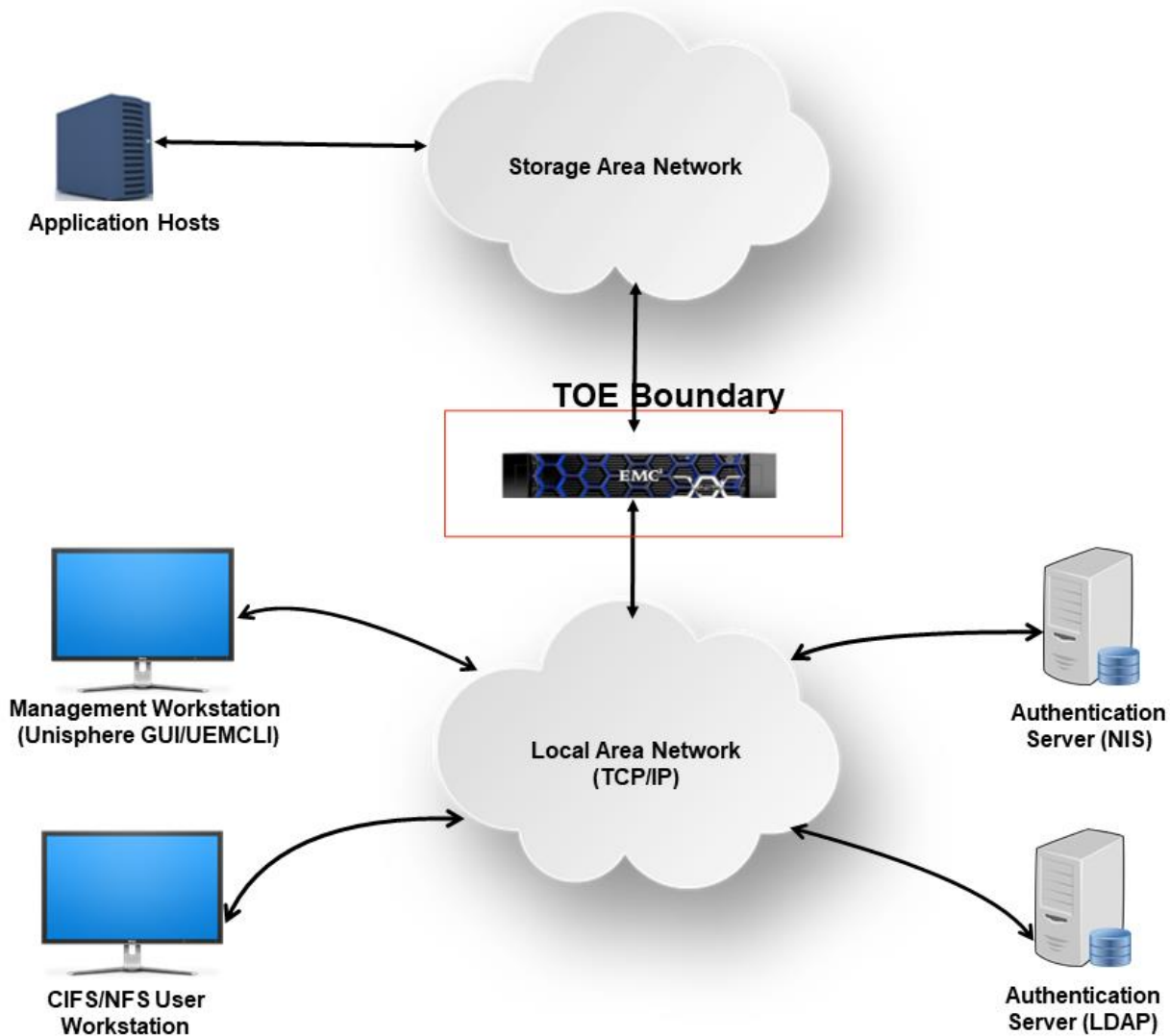


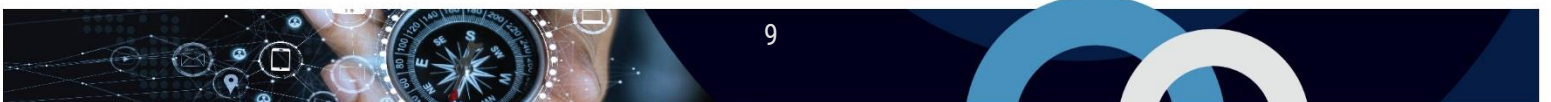
Figure 1: TOE Architecture

2 SECURITY POLICY

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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels

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



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 attributes used by the TOE to make File Storage Access Control decisions are provided by the operational environment.
- The TOE is located within controlled access facilities, which will prevent unauthorized physical and logical access.
- The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

3.2 CLARIFICATION OF SCOPE

The following functions are outside of the logical TOE scope and have not been evaluated:

- Data at Rest Encryption (D@RE)
- Common Event Enabler (CEE)
- File-level retention
- Replication
- EMC Secure Remote Services support (ESRS)
- UnityVSA
- CloudIQ (Unity Cloud Edition)
- vStorage API for Storage Awareness (VASA)

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software/Firmware	Unity Operating Environment 5.2.0.0.5.173 Unisphere 5.2.0.0.5.173 Unisphere CLI version 5.2.0.1642972
TOE Hardware	Unity 380/380F Unity 480/480F Unity 680/680F Unity 880/880F
Environmental Support	Authentication Server (NIS or LDAP)

4.1 DOCUMENTATION

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

- Dell EMC Dell EMC Unity OE v5.2 Common Criteria Guide Version 1.1 December 2022
- Online documentation at the Dell Unity Info Hub:

<https://www.dell.com/support/kbdoc/en-us/000126652/dell-emc-unity-info-hub-product-documents-and-information>

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 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 tests, and performing a vulnerability analysis.

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 TESTING

During this evaluation, the evaluator developed independent functional & penetration 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. Interoperability Testing: The evaluator tested secure channel operation with a known-good implementation.
- c. Password Policy Testing: The evaluator verified password policy across multiple interfaces.
- d. Access Control Testing: The evaluator attempted to execute a command without authorization.

6.3.1 INDEPENDENT TESTING RESULTS

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



6.4 VULNERABILITY ANALYSIS

The vulnerability analysis 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 vulnerability analysis.

Type 1 & 2 searches were conducted on **26 September 2022** and included the following search terms:

Dell EMC Unity	OpenSLP	Log4j
Unisphere	OpenSSL	
Apache Tomcat	VASA	

Vulnerability searches were conducted using the following sources:

NIST National Vulnerability Database https://nvd.nist.gov	CISA – Known exploited vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog
Dell Security Advisories and Notices https://www.dell.com/support/security/en-ca/	OpenSSL Vulnerabilities https://www.openssl.org/news/vulnerabilities-1.1.0.html

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.



7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

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.

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
CCTL	Common Criteria Testing Laboratory
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
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
VASA	vStorage API for Storage Awareness

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.
Dell EMC Unity OE v5.2 Security Target, v1.5, 9 December 2022
Dell EMC Unity OE v5.2 Evaluation Technical Report, v1.1, 13 December 2022