



Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR **CYBER SECURITY**

COMMON CRITERIA CERTIFICATION REPORT

Tripwire Enterprise, Version 8.8.2.2

3 September 2020

500 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.....	12
5 Evaluation Analysis Activities	13
5.1 Development.....	13
5.2 Guidance Documents.....	13
5.3 Life-Cycle Support	13
6 Testing Activities	14
6.1 Assessment of Developer tests.....	14
6.2 Conduct of Testing	14
6.3 Independent Functional Testing	14
6.3.1 Functional Test Results.....	14
6.4 Independent Penetration Testing.....	15
6.4.1 Penetration Test results.....	15
7 Results of the Evaluation	16
7.1 Recommendations/Comments.....	16
8 Supporting Content.....	17
8.1 List of Abbreviations.....	17



8.2 References.....18

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 Tripwire Enterprise, Version 8.8.2.2 (hereafter referred to as the Target of Evaluation, or TOE), from Tripwire, Inc. , 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 3 September 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 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 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	Tripwire Enterprise, Version 8.8.2.2
Developer	Tripwire, Inc.

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 intrusion detection system consisting of a sensor, scanner, and analyzer to monitor IT systems for activity that may indicate inappropriate activity on the IT system. The TOE is a software-only TOE. The Tripwire Enterprise server runs on various operating systems, including the Windows and Red Hat Enterprise Linux operating systems included in this evaluation.



1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

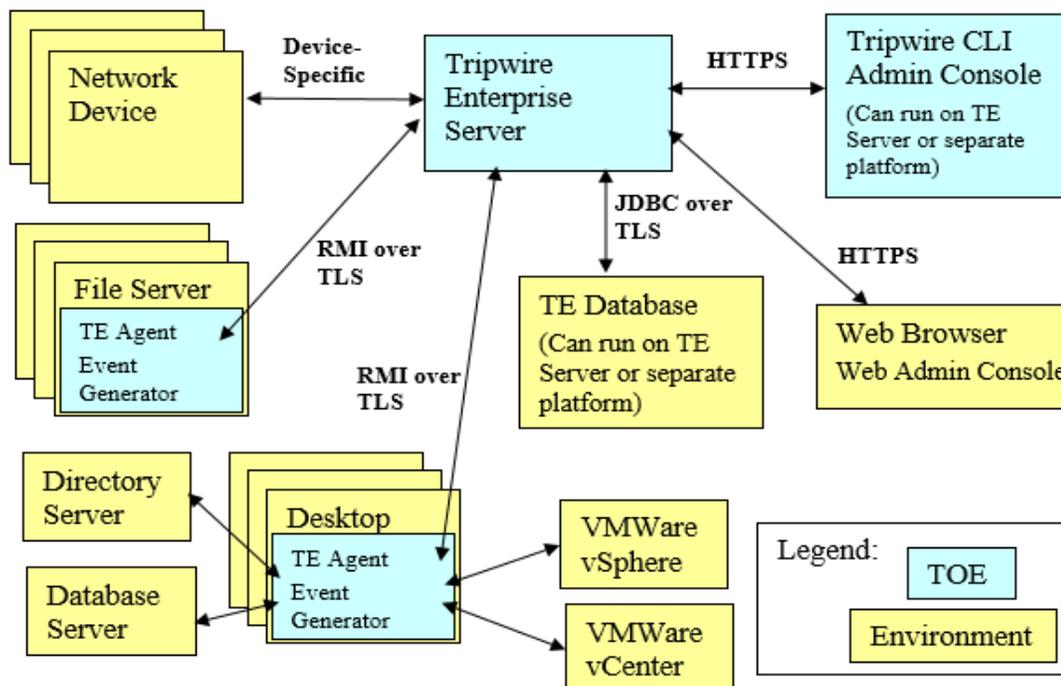


Figure 1: TOE Architecture

2 SECURITY POLICY

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

- Intrusion Detection System (IDS)
- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

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 implementations have been evaluated by the CMVP and are used by the TOE:

Table 2: Cryptographic Implementation(s)

Cryptographic Module/Algorithm	Certificate Number
OpenSSL FIPS Object Module SE v2.0.16	2398
BC-FJA (Bouncy Castle FIPS Java API) v1.0.1	3152

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:

- **Intended Usage Assumptions:** The TOE has access to all the IT System data it needs to perform its functions. The TOE is appropriately scalable to the IT System the TOE monitors. The TOE will be managed in a manner that allows it to appropriately address changes in the IT Systems the TOE monitors.
- **Physical Assumptions:** The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- **Personnel Assumptions:** 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, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The TOE can only be accessed by authorized users.

3.2 CLARIFICATION OF SCOPE

The following features are excluded from the scope of the evaluation:

- The Evaluated Configuration of the TOE does not include the Remedy AR System tickets Plugin, the HP Openview Plug-in, or the AAA Monitoring Tool. The Remedy AR System tickets Plug-in and the HP Openview Plug-in are extra tools available from Tripwire. The guidance documentation instructs that these tools not be installed. The AAA Monitoring Tool is included within the TOE delivery.
- The ability to transfer logs is excluded from the evaluated configuration. This capability requires the use of the Tripwire Log Center. The guidance documentation instructs that this capability not be configured.
- The ability to use the set command to specify the default userid and password during a CLI session is excluded from the evaluated configuration via providing guidance instructing administrators to not use the set command.
- The Tripwire Configuration Datamart (AKA Arena) is licensed separately and is excluded from the TOE.
- Dynamic Software Reconciliation (DSR) is an external tool that operates as a client of the SOAP API. DSR is an optional add-on and is excluded from the TOE.
- The Tripwire Enterprise Common Agent Platform (CAP), including the Security Content Automation Protocol (which is a CAP agent) is excluded from the TOE.
- Using Tripwire Enterprise Agents to monitor directory servers or database servers is excluded from the TOE.
- Configurator functionality is available only when Tripwire Enterprise itself is not running.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- Tripwire Enterprise, Version 8.8.2.2 (Build number r20200327101201-e056196.b20) server running on the following operating systems:
 - Windows Server 2016
 - Windows Server 2019
 - Red Hat Enterprise Linux 8.0
 - Red Hat Enterprise Linux 7.6
- Java Agent 8.7.3.1 (Build Number: r20200212093221-e1c4b0a.b22), Axon Agent 8.8.0.3 (Build Number: r20200306184815-4423b33.b2950), running on the following operating systems.
 - RedHat Enterprise Linux version 8.0
 - RedHat Enterprise Linux version 7.6
 - Microsoft Windows 10
 - Microsoft Windows Server 2016
 - Microsoft Windows Server 2019
 - Amazon Linux 2015.09 (4.1.17-22.30)

With support from the environment for:

- Java Virtual Machine –provides a runtime environment for the TOE.
- SMTP Server –An email server is used to facilitate delivery of integrity check results to administrators when the TOE is so configured.
- SNMP recipient –A network management device is used to facilitate delivery of integrity check results to administrators when the TOE is so configured.
- Syslog Server –A destination for the collection of log messages sent by the TOE.
- Workstation providing a web browser for access to the GUI.
- Tripwire Enterprise Nodes.
- LDAP/Active Directory server –An authentication server used to authenticate Tripwire Enterprise users when the System Login Method is set to LDAP/Active Directory.

4.1 DOCUMENTATION

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

- a) Tripwire Enterprise v8.8.2 Reference Guide, 23 April 2020.
- b) Tripwire Enterprise v8.8.2 User Guide, 23 April 2020.
- c) Tripwire Enterprise v8.8.2 Installation and Maintenance Guide, 23 April 2020.
- d) Tripwire Enterprise 8.8.2 Console Release Notes, December 2019
- e) Tripwire Enterprise v8.8.2 Hardening Guide, 23 April 2020.
- f) Tripwire Enterprise v8.8.2.2 Supplemental Common Criteria Guidance, 30 June 2020.
- g) Tripwire Enterprise Agent and Tripwire Axon Agent Release Notes, April 2020

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 claimed implementation was present and used by the TOE.
- c. Identification and Authentication: The objective of this test goal is to ensure that the identification and authentication requirements have been met.
- d. Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed.
- e. Users and Roles: The objective of this test goal is to ensure the users and roles functionality is correct.
- f. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data.
- g. Basic Product Functionality: The objective of this test goal is to exercise the TOE's functionality to ensure that the security claims may not be inadvertently compromised.

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 6/30/2020 and included the following search terms:

- Tripwire
- Tripwire Enterprise

Vulnerability searches were conducted using the following sources:

- National Vulnerability Database: <https://nvd.nist.gov/vuln/search>
- TripWire support: <https://www.tripwire.com/support/>
- Common Vulnerabilities and Exposures: <https://cve.mitre.org/cve/>

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



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
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
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.
Tripwire, Inc. Tripwire Enterprise Version 8.8.2.2 Security Target, Version 1.0, 12 August 2020.
Evaluation Technical Report for Common Criteria Evaluation of Tripwire, Inc. Tripwire Enterprise, Version 8.8.2.2, Version 1.1, 03 September 2020.

