Communications Security Establishment
Centre de la sécurité des télécommunications

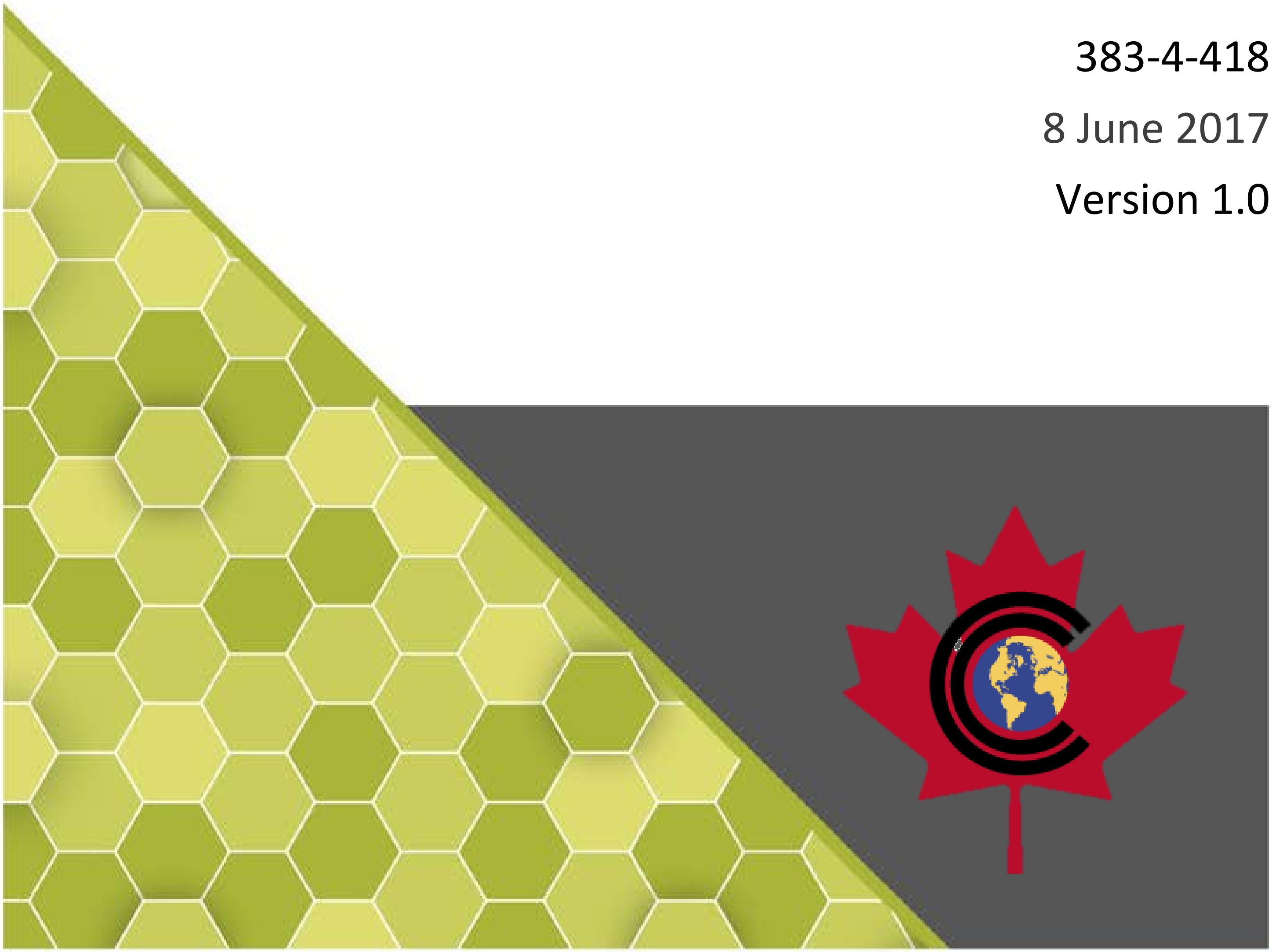
COMMON CRITERIA CERTIFICATION REPORT

Shavlik U.S Federal Protect Standard v9.2 Update 3

383-4-418

8 June 2017

Version 1.0



Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at 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 Common Criteria Scheme – 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, 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 the Communications Security Establishment, 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, 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:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

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 Communications Security Establishment.

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 17025:2005, 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 DXC Security Testing/Certification 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 posted to the Certified Products list (CPL) for the Canadian CC Scheme and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Shavlik U.S Federal Protect Standard v9.2 Update 3 (hereafter referred to as the Target of Evaluation, or TOE), from Ivanti, 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 TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE provides patch management, asset inventory, scripts for IT management and Information Assurance Vulnerability Alert (IAVA) reporting. These functions combine to provide an IT management solution that supports efforts to keep all machines up-to-date and protected from vulnerabilities.

Patch management allows for all Windows-based machines and VMware ESXi hypervisors in the network to be scanned. Once scanned, a report detailing the un-patched software vulnerabilities on the network is generated. Based on the scan results, schedules may be created to download and deploy missing patches. E-mail alerts providing patch availability, deployment status, and scan results may be sent to IT personnel to help streamline processes and ensure each machine is up-to-date. Patch management may be performed with or without agents.

DXC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 08 June 2017 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.

Communications Security Establishment, as the Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Canadian Certified Products list (CPL) 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	Shavlik U.S Federal Protect Standard v9.2 Update 3
Developer	Ivanti
Conformance Claim	EAL 2+ (ALC_FLR.2)

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.

1.2 TOE DESCRIPTION

The TOE provides patch management, asset inventory, scripts for IT management and Information Assurance Vulnerability Alert (IAVA) reporting. These functions combine to provide an IT management solution that supports efforts to keep all machines up-to-date and protected from vulnerabilities.

Patch management allows for all Windows-based machines and VMware ESXi hypervisors in the network to be scanned. Once scanned, a report detailing the un-patched software vulnerabilities on the network is generated. Based on the scan results, schedules may be created to download and deploy missing patches. E-mail alerts providing patch availability, deployment status, and scan results may be sent to IT personnel to help streamline processes and ensure each machine is up-to-date. Patch management may be performed with or without agents.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

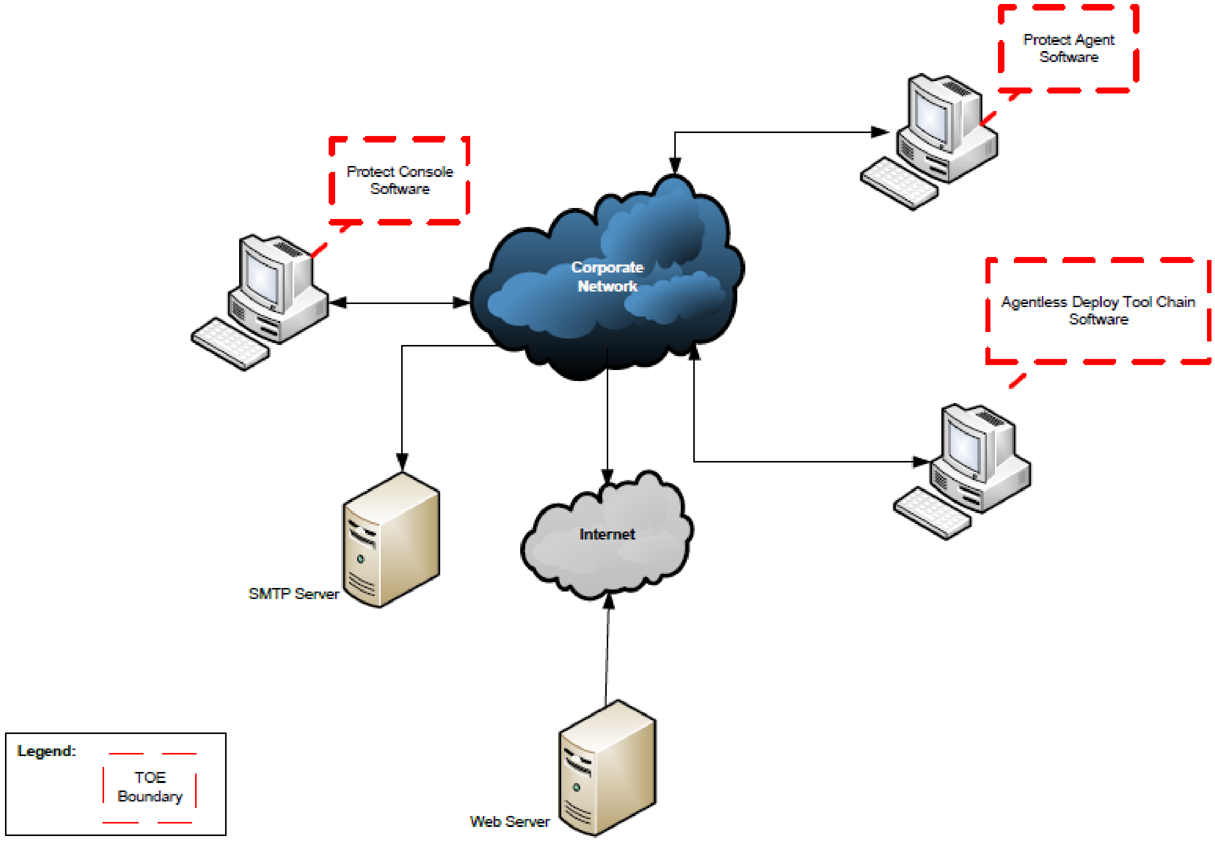


Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Security Audit;
- User Data Protection;
- Identification and Authentication;
- Security Management;
- Protection of the TSF;
- Resource Utilization; and
- Data Collection.

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

3 ASSUMPTIONS AND CLARIFICATIONS 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:

- FIPS 140-2 validated cryptographic algorithms in the TOE environment must provide all cryptographic functionality for the TOE;
- All ports needed for proper operation of the TOE will be opened at the firewall. Also, any firewall settings necessary for the TOE's operation will be configured to allow the TOE to operate;
- The Protect Console is installed on a server running Windows Server 2012 or Windows Server 2012 R2 that is dedicated to the TOE and its Distribution Server;
- The TOE is located within a controlled access facility;
- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains;
- The TOE environment provides the network connectivity required to allow the TOE to provide secure patch management functions;
- The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance;
- The TOE environment is in a secure state and provides a sufficient level of protection to itself and the TOE components;
- The TOE environment will provide identification and authentication functions for users attempting to manage and use the TOE;
- The environment provides a sufficient level of protection to secure communications between Distribution Servers (if deployed), agents (if deployed), and other TOE components; and
- The TOE environment provides the TOE with the necessary reliable timestamps.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE, Shavlik U.S Federal Protect Standard v9.2 Update 3, comprises:

- Protect Console, build number 5119;
- Protect Agent; and
- Protect Deploy Tool Chain (including the Protect Scheduler service).

4.1 DOCUMENTATION

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

- Shavlik Protect Installation and Setup Guide 9.2;
- Shavlik Protect Upgrade Guide 9.2;
- Shavlik Protect Administration Guide 9.2;
- Shavlik Protect Quick Start Guide 9.2;
- Shavlik Protect Agent Quick Start Guide 9.2;
- Shavlik Protect Virtual Machines Quick Start Guide 9.2;
- Shavlik Protect Best Practices Guide 9.2;
- Shavlik Protect Migration Tool User’s Guide 9.2;
- Shavlik Protect Report Views Guide 9.2;
- Supported Products 9.2 List; and
- U.S. Federal Protect Standard v9.2 Update 3 Guidance Documentation Supplement.

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, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). 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.

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

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 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 developers tests;

b. Security Roles: The objective of this test goal is to verify the user role assignments and verify the TOE identifier;

c. Machine Group: The objective of this test goal is to verify that the TOE properly captures and records audit information of machines scanned and patched;

d. Start up and shut down: The objective of this test goal is to verify that start up and shut down operations are properly recorded in the audit file;

e. Access Control: The objective of this test goal is to verify that role based access control performs as stated;

f. Email Notification and Resource utilization: The objective of this goal verifies the resource utilization capabilities of the TOE plus the ability to be notified by email;

g. Patch Deployment Roll Back: The objective of this test goal is to verify the TOE's capabilities for patch deployment and roll back; and

h. Import and Export: The objective of this test goal is to verify the TOE's capability of importing and exporting digitally signed patch files.

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

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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST;

b. Agent GUI: The objective of this test goal is to confirm that local administrators are not permitted to interact with the TSF;

c. Inter TOE Communication: The objective of this test goal is to determine if inter-TOE communication is appropriately protected; and

d. TOE Self-Test: The objective of this test goal is to verify that the TOE runs a series of self-tests during the execution of a TOE process.

6.4.1 PENETRATION TEST RESULTS

The independent penetration testing did not uncover any 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 IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

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 CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE 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
CPL	Canadian Certified Products List
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GC	Government of Canada
IAVA	Information Assurance Vulnerability Alert
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories – Canada
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 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Shavlik U.S. Federal Protect Standard v9.2 Update 3 Security Target, version 0.3, October 25, 2016
Evaluation Technical Report Shavlik U.S. Federal Protect Standard v9.2 Update 3, version 1.0, June 8, 2017