Certification Report

US Federal Shavlik Protect Standard v9.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-283-CR
Version:	1.0
Date:	4 December 2014
Pagination:	i to iii, 1 to 10

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, 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 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, 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.

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.

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 CSC Security Testing/Certification Laboratories.

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 4 December 2014, 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).

- Shavlik is a registered trademark of Shavlik.

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

TABLE OF CONTENTS

Executive Summary

US Federal Shavlik Protect Standard v9.1 (hereafter referred to as Shavlik Protect Standard), from Shavlik, is the Target of Evaluation. The results of this evaluation demonstrate that Shavlik Protect Standard meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Shavlik Protect Standard provides patch management, asset inventory, scripts for IT management and Information Assurance Vulnerability Alert (IAVA) reporting. These functions combine to provide a centralized IT management solution that supports keeping all machines up to date and protected from vulnerabilities.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 4 December 2014 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 Shavlik Protect Standard, 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 CCS Certification Body, declares that the Shavlik Protect Standard 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).

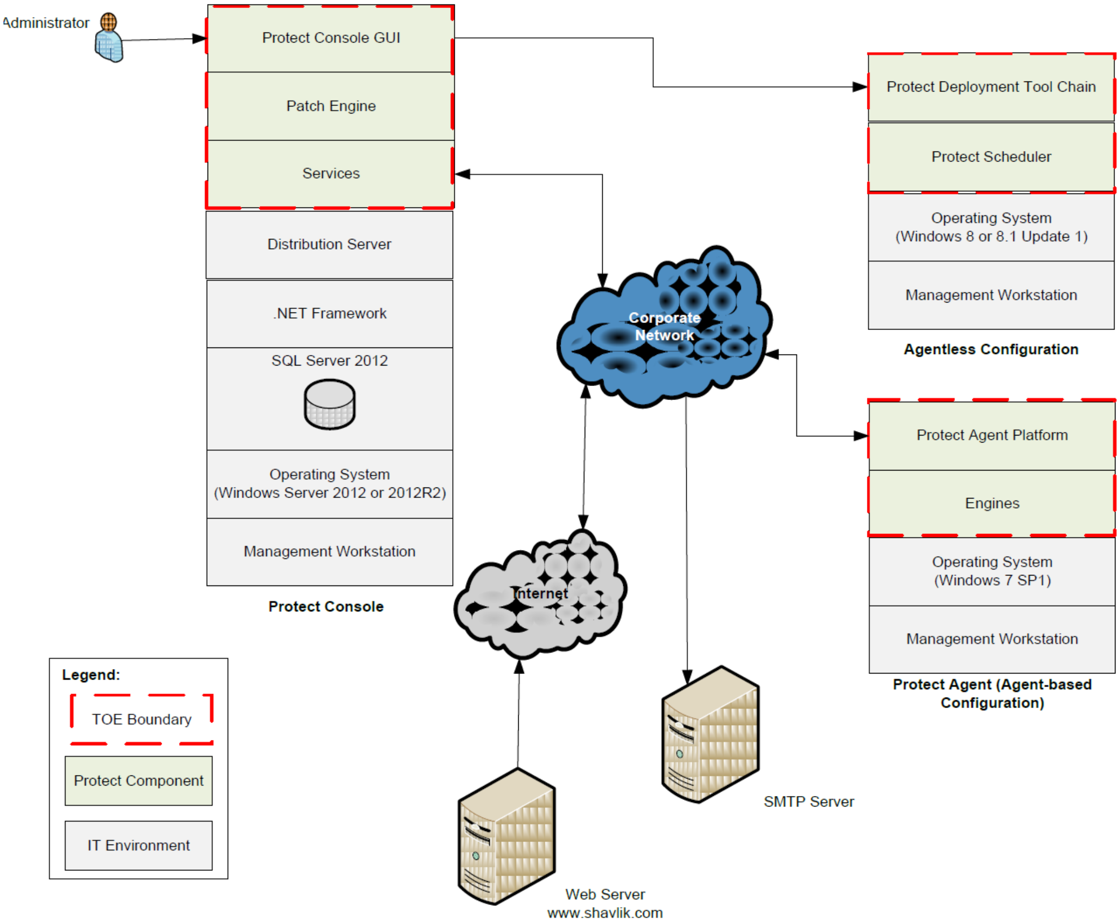
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is US Federal Shavlik Protect Standard v9.1 (hereafter referred to as Shavlik Protect Standard), from Shavlik.

2 TOE Description

Shavlik Protect Standard provides patch management, asset inventory, scripts for IT management and Information Assurance Vulnerability Alert (IAVA) reporting. These functions combine to provide a centralized IT management solution that supports keeping all machines up to date and protected from vulnerabilities.

A diagram of the Shavlik Protect Standard architecture is as follows:



3 Security Policy

Shavlik Protect Standard implements a role-based access control policy to control administrative access to the system. In addition, Shavlik Protect Standard implements policies pertaining to the following security functional classes:

Security Audit;

User Data Protection;

Identification and Authorization;

Security Management;

Protection of the TSF;

Resource Utilization; and

Data Collection.

4 Security Target

The ST associated with this Certification Report is identified below:

Shavlik U.S. Federal Shavlik Protect Standard v9.1 Security Target, v0.6, November 21, 2014.

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.*

Shavlik Protect Standard is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following:*
   - ALC_FLR.2
b. *Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:*
   - FDC_ANA.1 – System Analysis;
   - FDC_SCN.1 – System Scan; and
   - FDC_STG.1 – Scanned Data Storage.
c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of Shavlik Protect Standard 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- A 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 TOE is installed on a Management Workstation running Windows 2012R2 dedicated to the TOE and its Distribution Server.
- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE environment provides the network connectivity required to allow the TOE to provide secure patch management functions.
- 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.
- The TOE environment provides the TOE with the necessary reliable timestamps.
- The TOE is located within a controlled access facility.

7 Evaluated Configuration

The evaluated configuration for Shavlik Protect Standard is software only and is comprised of:

- U.S. Federal Shavlik Protect Standard v9.1, Build 9.1.4472.0.

which is installed on general-purpose computing hardware running the Microsoft Windows OS.

The publication entitled Shavlik Protect Installation and Setup Guide 9.1, *describes the procedures necessary to install and operate Shavlik Protect Standard in its evaluated configuration.*

8 Documentation

The Shavlik documents provided to the consumer are as follows:

- Online Help
- Shavlik Protect Installation and Setup Guide 9.1, 20 April 2014
- Shavlik Protect Upgrade Guide 9.1,
- Shavlik Protect Administration Guide 9.1, 20 April 2014
- Shavlik Protect Quick Start Guide 9.1, 20 April 2014
- Shavlik Protect Agent Quick Start Guide 9.1, 20 April 2014
- Shavlik Protect Virtual Machines Quick Start Guide 9.1,
- Shavlik Protect Best Practices Guide 9.1
- Shavlik Protect Migration Tool User’s Guide 9.1
- Shavlik Protect Report Views Guide 9.1
- Supported Products 9.1 List and,
- US Federal Shavlik Protect Standard v9.1 Guidance Documentation Supplement v0.5

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Shavlik Protect Standard, including the following areas:

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

The evaluators reviewed the flaw remediation procedures used by developer for the Shavlik Protect Standard. 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.

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

10 ITS Product Testing

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

10.1 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[1].

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.

10.2 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. Resulting from this test coverage approach is the following list of 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. Security Roles: The objective of this test goal is to verify user role assignment;

c. Create Machine Group, Perform Scan and View Audit: The objective of this test goal is to verify that the TOE captures audit information of machines scanned, patches deployed and security violations;

d. Start up and shut down of audit: The objective of this test goal is to verify that the start-up and shut down of the protect console service will generate an audit in the event viewer;

e. Access Control: The objective of this test goal is to verify the role based access controls;

f. Resource Utilization: The objective of this test goal is to verify resource utilization capabilities through the setting of the number of scans to be performed;

g. TSF Integrity: The objective of this test goal is to verify that the TOE’s executables are digitally signed;

h. Patch Deployment Rollback: The objective of this test goal is to verify the capabilities of the patch deployment and rollback;

i. Patch Deployment Signature Verification: The objective of this test goal verifies the signature verification performed by the TOE During Patch Deployment; and

[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.

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

10.3 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:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

b. SQL Bypass of RBAC: The objective of this test goal is to attempt to bypass the Protect Console through authorized access at the application database;

c. Agent GUI: The objective of this test goal is to verify that local administrators on target machine cannot interact with the TSF; and

d. Inter-TOE Communication: The objective of this test goal verifies that inter-TOE Communication is appropriately protected.

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

10.4 Conduct of Testing

Shavlik Protect Standard 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 Facility. 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.

10.5 Testing Results

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

11 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.

12 Evaluator Comments, Observations and Recommendations

The evaluator found U.S. Federal Shavlik Protect Standard v9.1 to be an intuitive patch and configuration management tool that provides robust security measures. The evaluator recommends that users follow the US Federal Shavlik Protect Standard v9.1 Guidance Documentation Supplement if they wish to deploy the evaluated configuration. Departure from the evaluated configuration should only be performed in consideration of the deployment scenario and associated risk profile.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

14 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. Shavlik U.S. Federal Shavlik Protect Standard v9.1 Security Target, v0.6, November 21, 2014.

e. Evaluation Technical Report Shavlik U.S. federal Shavlik Protect Standard v9.1, v1.9, December 4, 2014.