Certification Report

HP Network Automation Ultimate Edition 10.10

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-327-CR
Version: 1.0
Date: 24 September 2015
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 CGI IT Security Evaluation & Test Facility.

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 24 September 2015, 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).

TABLE OF CONTENTS

Executive Summary

HP Network Automation Ultimate Edition 10.10 (hereafter referred to as HP Network Automation 10.10), from Hewlett Packard Enterprise Development LP, is the Target of Evaluation. The results of this evaluation demonstrate that HP Network Automation 10.10 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

HP Network Automation 10.10 is a centralized infrastructure management and policy enforcement solution that tracks and regulates network device configuration changes across routers, switches, firewalls, load balancers, and wireless access points. The TOE discovers network devices and retrieves and stores each device's current configuration information. The TOE provides all of the management and policy compliance functionality in addition to locally discovering devices connected to the same network.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 24 September 2015 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 HP Network Automation 10.10, 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 HP Network Automation 10.10 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 HP Network Automation Ultimate Edition 10.10 (hereafter referred to as HP Network Automation 10.10), from Hewlett Packard Enterprise Development LP.

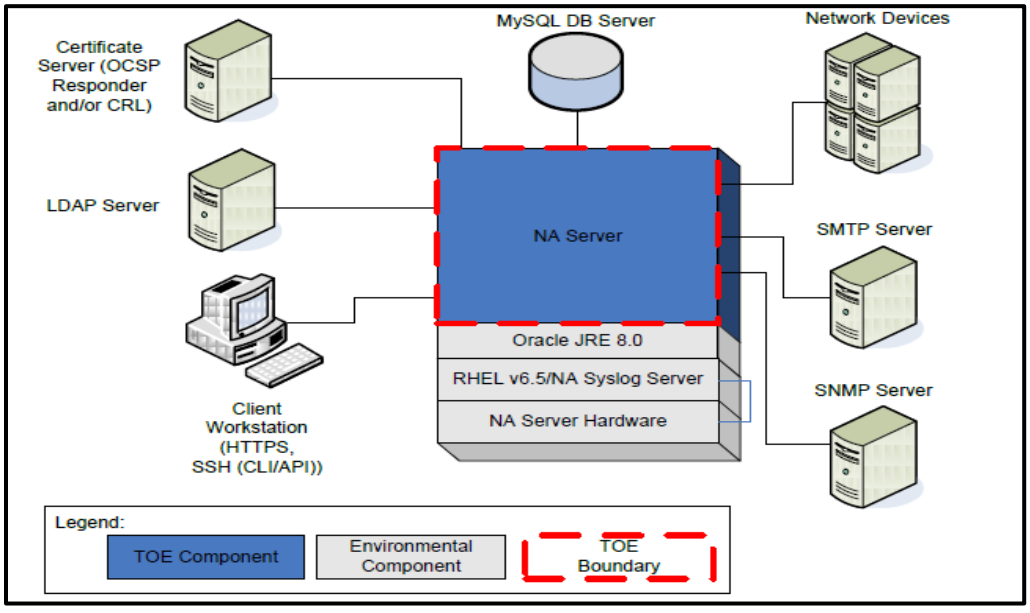
2 TOE Description

The TOE is a centralized infrastructure management and policy enforcement solution that tracks and regulates network device configuration changes across routers, switches, firewalls, load balancers, and wireless access points. The TOE discovers network devices and retrieves and stores each device's current configuration information.

The TOE provides a web-based graphical user interface (GUI) and a Command Line Interface (CLI)/Application Programing Interface (API) that can be used by administrators to manage policies and rules, create and edit user accounts, review audit logs, and manage cryptographic functionality.

The TOE uses a FIPS-validated cryptographic module to provide a secure connection with the web GUI using HTTPS (via TLS) and with the CLI/API using SSH. For device discovery and configuration snapshots the TOE can connect to remote devices in the operational environment over a trusted channel using SSH.

A diagram of the HP Network Automation 10.10 architecture is as follows:



3 Security Policy

HP Network Automation 10.10 implements a role-based access control policy to control administrative access to the system. In addition, HP Network Automation 10.10 implements policies pertaining to the following security functional classes:

- *Security Audit*
- *Cryptographic Support*
- *Identification and Authentication*
- *Security Management*
- *TOE Access*
- *Trusted path/channels*
- *Network Automation Support*

The following cryptographic module was evaluated to the FIPS 140-2 standard:

Cryptographic Module	Certificate
RSA B-SAFE Crypto-J JSAFE and JCE Cryptographic Library version 6.1	2057

4 Security Target

The ST associated with this Certification Report is identified below:

Hewlett Packard Enterprise Development LP Network Automation Ultimate Edition v10.10 Security Target, Version 0.13, September 22, 2015.

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.

HP Network Automation 10.10 is:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following:
    - ALC_FLR.2 - Flaw Reporting Procedures
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:
    - EXT_NAS_DCD.1 - Device and Configuration Discovery
    - EXT_NAS_NCE.1 - Non-Compliance Events
    - EXT_NAS_PCM.1 - Policy Compliance
    - EXT_NAS_RDR.1 - Restricted Data Review
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 HP Network Automation 10.10 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 Assumption is listed in the ST:

- Administrators are non-hostile, appropriately trained, and follow all administrator guidance.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is installed on the appropriate, dedicated hardware and operating system.
- The TOE and the connections between the TOE and TOE environmental components (the MySQL DB Server) are located within a controlled access facility on a secured network.
- The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.
- The TOE software will be protected from unauthorized modification.
- The TOE environment will provide the TOE with the necessary reliable timestamps.

7 Evaluated Configuration

The evaluated configuration for HP Network Automation 10.10 comprises the HP Network Automation 10.10 software installed on Network Automation hardware running RHEL 6.5.

The following environmental components are required for the proper operation of the TOE in the evaluated configuration:

- Client workstation used to connect to the TOE, installed with Mozilla Firefox or Internet Explorer
- SSH client
- Authentication Server to support LDAP external authentication requests
- Certificate Server configured for X.509 certificates
- MySQL Database Server version 5 or newer
- Oracle JRE 8.0
- Network Automation syslog server
- Actively monitored network devices
- SNMP server
- SMTP server

The publication entitled *HP Network Automation Ultimate Edition v10.10 Guidance Supplement v0.6* describes the procedures necessary to install and operate HP Network Automation 10.10 in its evaluated configuration.

8 Documentation

The Hewlett Packard Enterprise Development LP documents provided to the consumer are as follows:

a. HP Network Automation Software Version 10.10, Installation and Upgrade Guide, June 2015;

b. HP Network Automation Software Version 10.10, Administrator Guide, June 2015;

c. HP Network Automation Software Version 10.10, User Guide, June 2015;

d. HP Network Automation Software (NA) CLI/API Command Reference, Software Version 10.10, June 2015; and

e. HP Network Automation Ultimate Edition v10.10 Guidance Supplement, Version 0.6

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of HP Network Automation 10.10, including the following areas:

Development: The evaluators analyzed the HP Network Automation 10.10 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 HP Network Automation 10.10 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 HP Network Automation 10.10 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 HP Network Automation 10.10 configuration management system and associated documentation was performed. The evaluators found that the HP Network Automation 10.10 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 HP Network Automation 10.10 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the HP Network Automation 10.10. 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. Policy Creation and Audit: The objective of this test goal is to confirm that an Administrator can create event, notification and response rules and that these actions are auditable;

c. Power User and Administrator Roles: The objective of this test goal is to confirm that the Power User role can log into the web GUI and view audit records and that the Administrator can log into the web GUI and create a new user;

d. Authentication failover: The objective of this test goal is to confirm that the TOE supports local authentication failover, allowing TOE operators to access the TOE when there is a problem with the external authentication server;

e. Access Control: The objective of this test goal is to verify that the TOE enforces access control permissions for administrative users of the TOE;

f. Audit review through CLI, Java API: The objective of this test goal is to verify that administrators with appropriate permissions can review audit records via through the CLI and the Java API;

g. Certificate based user authentication: The objective of this test goal is to verify that the TOE supports certificate based user authentication; 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.

h. Receiving Interface Testing: The objective of this test goal is to verify that the TOE can discover a network device and receive configuration information concerning that device.

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. Cookie Strength: The objective of this test is to determine whether the TOE is susceptible to weak session IDs;

c. Session Fixation: The objective of this test is to determine whether an attacker can hijack a valid user session;

d. Weak Algorithms in SSL/TLS: The objective of this test is to determine whether the TOE accepts weak algorithms for SSL/TLS; and

e. Weak Algorithms in SSH: The objective of this test is to determine whether the TOE accepts weak algorithms for SSH.

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

10.4 Conduct of Testing

HP Network Automation 10.10 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.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that HP Network Automation 10.10 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
API	Application Programming Interface
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
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

13 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. Hewlett Packard Enterprise Development LP Network Automation Ultimate Edition v10.10 Security Target, Version 0.13, September 22, 2015.

e. Hewlett Packard Enterprise Development LP Network Automation 10.10 Common Criteria EAL2 Evaluation Technical Report Version 1.1, September 24, 2015.