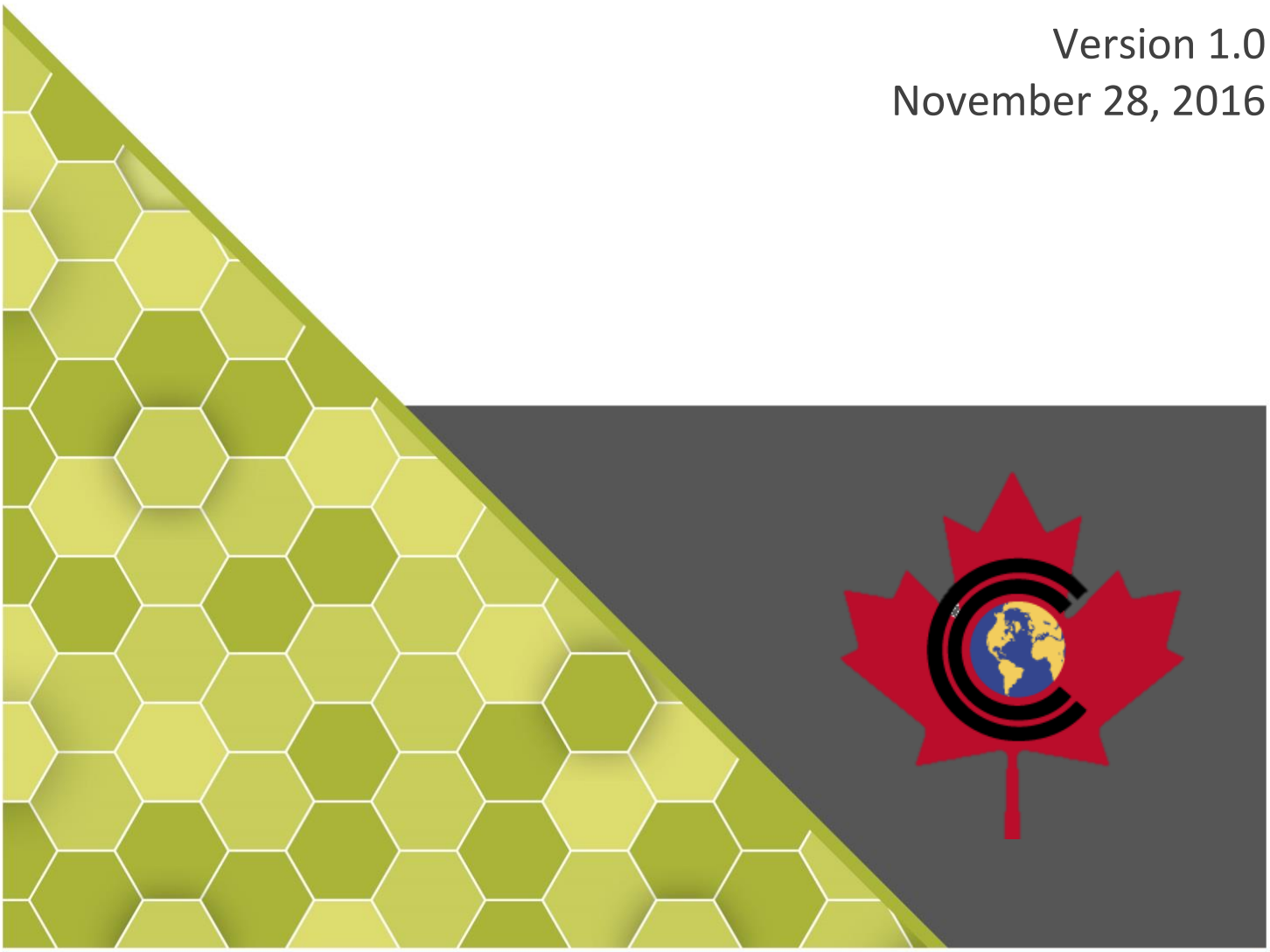
COMMON CRITERIA MAINTENANCE REPORT

NetIQ® Secure Configuration Manager™ 6.2.0

Version 1.0
November 28, 2016



Canada

FOREWORD

The *Document Name* 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.

If your department has identified a requirement for 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

EWA Canada has submitted the Impact Analysis Report (IAR) for NetIQ® Secure Configuration Manager™ 6.2.0 (hereafter referred to the TOE), satisfying the requirements outlined in Assurance Continuity: CCRA Requirements, v2.1, June 2012. In accordance with those requirements, the IAR describes the changes implemented in the TOE, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

TABLE OF CONTENTS

1 CHANGES

The following characterizes the changes implemented in the TOE and/or the environment. For each change, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted by the developer to ensure that the assurance in the Target of Evaluation (TOE) was maintained.

1.1 DESCRIPTION OF CHANGES IN THE MAINTAINED TARGET OF EVALUATION

The changes in the TOE comprise;

- bug fixes and feature enhancements resulting from defects detected and resolved through the QA/test process that do not affect the existing security features of the of TOE;
- Secure Configuration Manager now closes the database connections after registering endpoints correctly;
- Secure Configuration Manager now retains report options even if the template is edited and updated;
- Exceptions can be edited at any time even if the template that is specified in the exception is run against a different group;
- When the missing patches assessment is run, the Windows Update service starts automatically and now does not revert to the stopped state after the missing patches assessment is complete;
- The new Agent Manager Connector addresses communication issues between the Security Agent for UNIX and the Sentinel server due to a mismatch of the hostname in the certificate;
- Secure Configuration Manager Dashboard users can now view only the data in the Dashboard for which they have permissions;
- Secure Configuration Manager 6.2 is enabled with SCAP version 1.2;
- Secure Configuration Manager Dashboard 6.2 includes a new chart called Check Status Distribution that displays the collective status of the security checks that have been run in the network;
- Secure Configuration Manager 6.2 includes new security checks for the security audit settings of the endpoint, for the enabling of IP forwarding, and for user accounts with weak passwords;
- Secure Configuration Manager 6.2 has enhanced security checks for generic registry reporting the key-value mapping as well as the numeric value of the registry key;
- Secure Configuration Manager 6.2 has security checks to validate multiple regular expressions against multiple files with file size support check now consuming user-defined comparator-delimiter values as well if they are not part of the regular expression;
- Secure Configuration Manager 6.2 has support for reports on individual checks that are run as part of templates to be sent to third-party SIEM solutions;
- Secure Configuration Manager 6.2 now provides auditing information about changes made to report options while running or scheduling a run of policy templates;
- The audit rules are now dynamically created based on the required criteria when policies are assigned to the agent and are dynamically destroyed when policies are unassigned;
- The Security Agent for UNIX 7.5 can now be installed in FIPS mode;
- The Security Agent for UNIX 7.5 can now be installed on all 64-bit platforms without any 32-bit library dependencies; and

- Open Enterprise Server (OES) rule group now monitors Linux auditing events generated by the Network Security Services (NSS) auditing engine on Open Enterprise Server computers using the Agent and the Agent reads the Open Enterprise Server events and forwards the events to Sentinel.

1.2 AFFECTED DEVELOPER EVIDENCE

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted for the TOE. The set of affected developer evidence was identified in the IAR.

Modifications to the security target were made to reflect the new product versions.

2 CONCLUSIONS

Through functional and regression testing of the TOE, assurance gained in the original TOE certification was maintained. As all of the changes to the maintained TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification 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 Evaluation and Certification 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.

2.1 REFERENCES

Reference
Assurance Continuity: CCRA Requirements, v2.1, June 2012
CCS Guide #6, Technical Oversight for Assurance Continuity of a Certified TOE, v1.6, May 2011.
Certification Report NetIQ® Secure Configuration Manager™ 5.9.1, version 1.0, November 28, 2014
NetIQ® Secure Configuration Manager™ 6.2 Security Target, version 0.1, November 17, 2016