Common Criteria Certification Report

NetApp E-Series and EF-Series with SANTricity v11.90R5

CAN-684-LSS

23 June 2026

v1.0

Communications Security Establishment Canada
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

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 testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). 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 Common Criteria Program, and the conclusions of the testing laboratory 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 organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security

Contact Centre and Information Services

contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

Overview

The Canadian Common Criteria Program provides a third-party evaluation service for evaluating the security of IT products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL 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 (ST). 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 ST, in addition to this certification report, 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 CCTL.

The certification report, certificate of product evaluation and ST are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

Executive Summary CAN-684-LSS

NetApp E-Series and EF-Series with SANTricity v11.90R5 (hereafter referred to as the Target of Evaluation, or TOE), from **NetApp, Inc.** , was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that the TOE meets the following conformance claim: **collaborative Protection Profile for Network Devices, v3.0e.**

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on **23 June 2026** and was conducted in accordance with the rules of the Canadian Common Criteria Program.

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 consider 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 for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

Identification of Target of Evaluation

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	NetApp E-Series and EF-Series with SANTricity v11.90R5
Developer	NetApp, Inc.

See the Evaluated Configuration section for more details on the evaluated configuration of the TOE.

Common Criteria Conformance

The evaluation was conducted using the following methodology:

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:

collaborative Protection Profile for Network Devices, v3.0e.

TOE Description

The TOE is a network device that provides networked storage for dedicated, high bandwidth applications like data analytics, video surveillance, and disk-based backup that need simple, fast, reliable SAN storage.

TOE Architecture

A diagram of the TOE architecture is as follows:

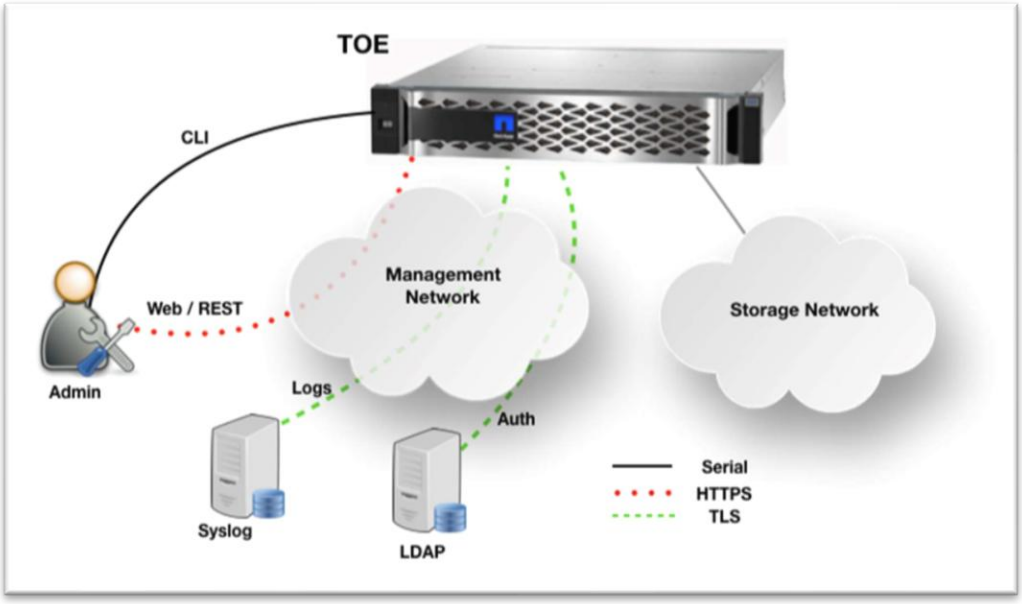

Figure 1: TOE Architecture

Security Policy

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

- Trusted Path/Channels
- Security Management
- Protection of the TSF
- Identification and Authentication
- TOE Access
- Security Audit
- Cryptographic Support

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

Cryptographic Functionality

The TOE makes use of the following CAVP validated cryptographic implementation:

Table 2: Cryptographic Implementation

Cryptographic Implementation	Certificate Number
NetApp, Inc. Bouncy Castle BC-FIPS version 11.90	A7093

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.

Usage and Environmental Assumptions

The following assumptions are made regarding the use and deployment of the TOE:

- The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result,the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption appliesto the physical platform on which the VM runs.
- The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
- A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
- The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

  For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

- The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
- The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Clarification of Scope

The SMcli client application is not included in the scope of the TOE evaluation.

Evaluated Configuration

The evaluated configuration for the TOE comprises:

Table 3: Evaluated Configuration

TOE Software/Firmware	SANtricity OS 11.90R5 Build11.90.00.9134
TOE Hardware	E4012 (DE212C), E4060 (DE460C), EF300, EF600, EF300C, EF600C
Environmental Support	Audit Server, LDAP Server, OCSP Responder

Documentation

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

a) E-Series and EF-Series w SANTricity v11.90R5 Common Criteria Guide, v1.3 June 22, 2026
b) EF300 and EF600 E-Series storage systems June 12, 2026
https://docs.netapp.com/us-en/e-series/pdfs/sidebar/EF300_and_EF600.pdf
c) NetApp Install hardware E-Series storage systems, June 12, 2026
https://docs.netapp.com/us-en/e-series/pdfs/sidebar/Install_hardware.pdf
d) NetApp E4000 E-Series storage systems, June 12, 2026
https://docs.netapp.com/us-en/e-series/pdfs/sidebar/E4000.pdf
e) NetApp Linux express configuration E-Series storage systems, June 12, 2026
https://docs.netapp.com/us-en/eseries/pdfs/sidebar/Linux_express_configuration.pdf
f) NetApp SANtricity System Manager SANtricity software, April 23, 2026
https://docs.netapp.com/us-en/e-series-santricity-119/pdfs/sidebar/SANtricity_System_Manager.pdf
g) NetApp Get Started SANtricity commands, March 17, 2026
https://docs.netapp.com/us-en/e-series-cli/pdfs/sidebar/Get_started.pdf

Evaluation Analysis Activities

The evaluation activities comprised a structured assessment of the TOE. Documentation and processes related to Development, Guidance Documentation, and Life-Cycle Support were reviewed and analyzed.

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.

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 exercised 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 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 the procedures required to maintain the integrity of the TOE during distribution to the consumer.

Testing Activities

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

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.

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 proprietary test results document.

Independent Testing

During this evaluation, the evaluator developed independent functional & penetration 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. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP; and
b. Validation of Cryptographic Implementation: The evaluator confirmed that the claimed cryptographic implementation is present in the TOE.

Independent Testing Results

The testing produced the expected results, supporting the conclusion that the TOE correctly implements the functional requirements specified in the ST and the TOE functional specification.

Vulnerability Analysis

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases, and technical community sources. Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities. Based upon this review, the evaluators formulated flaw hypotheses, which they used in their vulnerability analysis.

Public domain searches were conducted on **25 May 2026** and included the following search terms:

SANTricity v11.90	E4012 (DE212C), E4060 (DE460C), EF300, EF600, EF300C, EF600C
Intel Xeon D-1715TER, Intel Xeon D-2164IT, Intel Xeon D2123IT	BouncyCastle-FIPS

Vulnerability searches were conducted using the following sources:

NetApp Security Advisories	NIST National Vulnerabilities Database (NVD)
Maven Repository	CISA - Known Exploited Vulnerabilities Catalog
CVE	

Vulnerability Analysis Results

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

Results of the Evaluation

The Information Technology product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

Recommendations/Comments

It is recommended that all guidance be followed to configure the TOE in the evaluated configuration.

Include any comments/recommendations provided the CCTL (For example in the ETR/AAR) if different from above.

Supporting Content

List of Abbreviations

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

References

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5.
NetApp E-Series and EF-Series w SANTricity v11.90 R5 Security Target, v1.8, June 22, 2026.
NetApp E-Series and EF-Series w SANTricity v11.90 R5, Evaluation Technical Report, Version 1.3, June 23, 2026.
NetApp E-Series and EF-Series w SANTricity v11.90 R5 Assurance Activity Report, Version 1.3, June 23, 2026.