National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

QuintessenceLabs Trusted Security Foundation 400, Version 3.2

Report Number: CCEVS-VR-VID11518-2025
Dated: May 22, 2025
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Daniel Faigin
Marybeth Panock
Seada Mohammed
The Aerospace Corporation

Common Criteria Testing Laboratory

Anthony Apted
Greg Beaver
Pascal Patin
Allen Sant
Kevin Zhang
Leidos Inc.
Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of QuintessenceLabs Trusted Security Foundation 400, v3.2 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in May 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant and meets the assurance requirements of the *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 ([5]).

The TOE is QuintessenceLabs Trusted Security Foundation 400, v3.2.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed PP and, when installed, configured, and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST ([7]).

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	QuintessenceLabs Trusted Security Foundation 400, Version 3.2
Security Target	QuintessenceLabs Trusted Security Foundation 400, Version 3.2 Security Target, Version 1.0, March 5, 2025
Sponsor & Developer	QuintessenceLabs Unit 11, 18 Brindabella Circuit Brindabella Business Park Canberra Airport, ACT 2609 Australia
Completion Date	May 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Anthony Apted Greg Beaver Pascal Patin Allen Sant Kevin Zhang
Validation Personnel	Daniel Faigin Seada Mohammed Marybeth Panock

3 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The TOE is QuintessenceLabs' (QLabs) Trusted Security Foundation (TSF[1]) 400, Version 3.2. QLabs Trusted Security Foundation is a network-based appliance providing centralized and vendor-neutral key and policy management capabilities that seamlessly integrate into any organization's infrastructure. Trusted Security Foundation manages keys over their full life cycle in accordance with NIST SP 800-57 and KMIP protocol standards. The Trusted Security Foundation TOE is being evaluated as a network device and therefore the key and policy management capabilities were not evaluated.

The evaluation covers the secure communication channels for key management services (KMIP); database transactions and replication; and with LDAP, SMTP, backup and external syslog servers. Additionally, the evaluation covers all TOE functionality supporting the claims in the collaborative Protection Profile for Network Devices (NDcPP) [5]. The security functionality specified in the NDcPP includes protection of communications between the TOE and external IT entities as mentioned above, identification and authentication of administrators, auditing of security-relevant events, ability to verify the source and integrity of updates to the TOE, protection of TSF data, and use of NIST-validated cryptographic mechanisms.

The TOE is a standalone network device with a hardware security module (HSM) providing capabilities for key management and policy enforcement.

For the purpose of this evaluation, the TOE is treated as a network device offering NIST validated cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to export audit records), protected using HTTPS/TLS and SSH.

Cryptographic functionality is performed by the TOE's HSM, Nettle, and OpenSSL in support of higher level protocols (TLS, SSH). The modules' FIPS-Approved cryptographic algorithms have obtained CAVP certificates.

The TOE audits security relevant events, stores audit records locally, and can be configured to forward its audit records to an external syslog server in the network environment. An administrator can configure the TOE to solicit time from an NTP server, and alternatively the administrator can manually set the TOE's time.

The TOE uses: TLS to protect syslog, LDAP, SMTP, KMIP and database traffic; offers a management UI protected by TLS/HTTPS; and provides a management Command Line Interface (CLI) protected by SSH.

Administrators are able to query the current version of the product software and manage the security functions of the TOE, including performing updates on the product. A published hash is used for protection of the update files.

The TOE provides self-tests to ensure the integrity and correct operation of the TOE.

The TOE is operated in 'Common Criteria Mode' configured via the web UI. This mode places the TOE in the evaluated configuration by imposing cryptographic restrictions; disabling watchdogs and other excluded functions; and turning on password restrictions.

[1] QuintessenceLabs refers to the TOE as "TSF" in its product documentation – for the sake of clarity, this abbreviation is not used

4 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 Security Audit

The TOE generates audit events associated with identification and authentication, management, updates, and user sessions. The TOE can store the events in a local log and export them to a syslog server using a TLS protected channel. The TOE protects stored audit records from unauthorized modification and deletion.

4.2 Cryptographic Support

The TOE provides CAVP certified cryptography in support of its SSH, TLS, and NTP implementations and for verifying TOE update packages. Cryptographic services include key management, random bit generation, symmetric encryption and decryption, digital signature, and secure hashing.

4.3 Identification and Authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of reading the login banner. The TOE authenticates a user's credentials (password, key) using a local mechanism provided by the TOE and supports external LDAP authentication. The TOE also provides X.509 certificate checking for its TLS connections.

4.4 Security Management

The TOE provides CLI, web-based UI, and RESTful API management interfaces that an administrator can access remotely via a network port. The CLI can also be accessed locally by directly connecting to the appliances via USB port. Remote connections to the management interface are protected with SSH for the CLI and HTTPS for web-based. The management interface is limited to the authorized administrator.

4.5 Protection of the TSF

The TOE implements various self-protection mechanisms. The TOE performs self-tests that cover the correct operation of the TOE. It provides functions necessary to securely update the TOE. It relies upon either manually provided time or an NTP server in its environment to ensure reliable timestamps. It encrypts sensitive data such as passwords and cryptographic keys stored within it.

4.6 TOE Access

The TOE terminates local and remote interactive sessions after a configurable period of inactivity. The TOE additionally provides the capability for administrators to terminate their own interactive sessions. The TOE can be configured to display an advisory and consent warning message before establishing a user session.

4.7 Trusted Path/Channels

The TOE protects interactive communication with remote administrators using SSH (for remote access to the CLI) and HTTPS (for remote access to the Admin UI and RESTful API).

The TOE protects communications with authorized external IT entities using TLS and SSH. The TOE uses TLS to protect communications with external syslog, LDAP, and SMTP servers and external KMIP clients. The TOE can also transmit or receive replicated information from an external copy of the product in its operational environment over TLS. The TOE uses SSH to transmit backup data to an external backup server.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- 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.
- 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).
- 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 NDcPP. 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 being 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.

5.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following document:
    - *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 ([6])
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in QuintessenceLabs Trusted Security Foundation 400, Version 3.2 Security Target, Version 1.0, March 5, 2025 ([7]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- QuintessenceLabs Common Criteria (CC) Evaluated Configuration Guidance, Version 1.0, March 26, 2025 [8]
- Advanced Administration Guide, TSF KMS 3.2, March 6, 2025 [9]
- Common Criteria CLI Guide, TSF KMS 3.2, March 14, 2025 [10]
- Getting Started Guide, TSF KMS 3.2, March 6, 2025 [11]
- User Guide, TSF KMS 3.2, March 6, 2025 [12]

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- QuintessenceLabs Trusted Security Foundation 400, Version 3.2 Test Report and Procedures For Network Device collaborative PP Version 2.2e, Version 1.0, April 14, 2025 [15].

A non-proprietary description of the tests performed and their results is provided in the following document:

- Assurance Activities Report for QuintessenceLabs Trusted Security Foundation 400, Version 3.2, Version 1.0, April 14, 2025.

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 ([5]).

The evaluation team devised a Test Plan based on the Test Activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 ([6]). The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from February 2024 through April 2025.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *collaborative Protection Profile for Network Devices* were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration including the Trusted Security Foundation 400 device, running software version 3.2.

The following figure depicts the test environment established for testing the TOE.

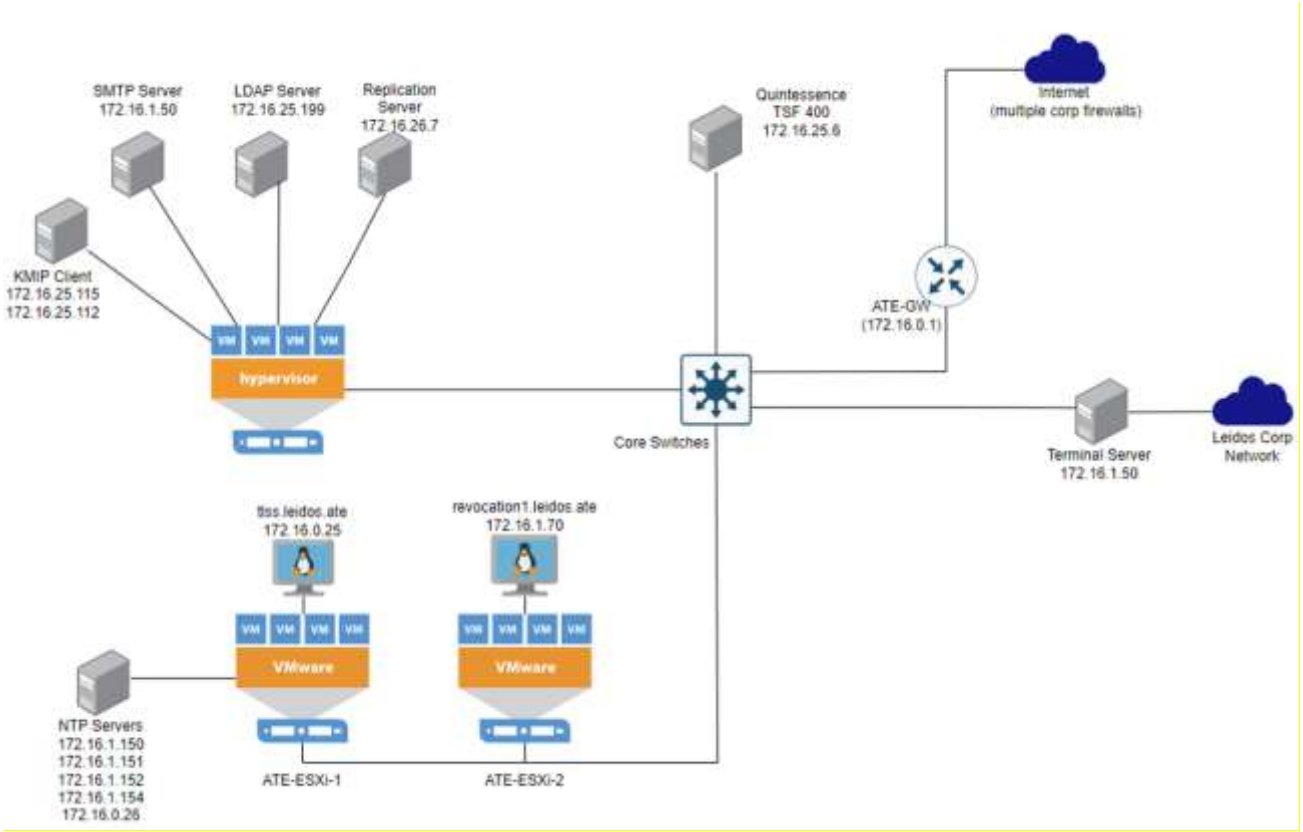

Figure 1: TOE Test Configuration

The test configuration included the following devices in the operational environment of the TOE:

- KMIP Client
- Replication Server
- SMTP Server
- LDAP Server
- Router/Gateway
- Terminal Server
- TLS Test Server
- Syslog Server
- NTP Servers

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is based on a Dell R6615 chassis with an AMD EPYC 9224 processor (Zen 4 microarchitecture) and runs on a purpose-build distribution of Red Hat Enterprise Linux (RHEL) 8.10. The TOE also includes the qStream 100 quantum random number generator and an Entrust nShield 5s hardware security module (HSM).

The TOE is placed into its evaluated configuration by enabling Common Criteria mode through its web UI as specified in the configuration guidance.

The TOE in its evaluated configuration may require the following components in its operational environment:

- Workstation that supports an SSH client or web browser
- Syslog server that stores audit records
- SMTP server that transmits configured email notifications
- LDAP server that is used for administrator authentication
- SSH server that can be used to receive backups
- KMIP clients that can be used to request key management services from the TOE
- Another instance of the Trusted Security Foundation 400 to or from which key material and metadata can be replicated

8.2 Excluded Functionality

The following features and capabilities of QuintessenceLabs Trusted Security Foundation 400, Version 3.2 are not covered by the evaluation:

- The Key Management Interoperability Protocol (KMIP) functionality of the product is outside the scope of the claimed Protection Profile; it is only tested to the extent that its communications occur over a TLS-protected channel.
- Any other product functionality referenced in operational guidance that is not explicitly referenced in the Security Target or Common Criteria Evaluated Configuration Guidance.
- The list below identifies features or protocols that are not evaluated or must be disabled, and the rationale why. Note that this does not mean the features cannot be used in the evaluated configuration (unless explicitly stated so). It means that the features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion. Evaluated functionality is scoped exclusively to the security functional requirements specified in this Security Target. In particular, only the following protocols implemented by the TOE have been tested, and only to the extent specified by the security functional requirements: TLS, HTTPS, SSH, NTP authentication. The features below are out of scope.

Table 2: Excluded Functionality

Feature	Description
OASIS KMIP, PKCS#11 over KMIP	The TOE supports OASIS Key Management, the PKCS#11 over KMIP protocol for its key and policy management functions. The [cPPND] does not define requirements for these protocols and functions and therefore they have not been evaluated.
Watchdog port	This provides a mechanism to monitor internal Trusted Security Foundation operations. This connection is not protected and is disabled in the evaluated configuration via setting 'Common Criteria Mode'.
Entropy portal	This provides an entropy service to enable external entities to retrieve random bytes. This service is accessed over an HTTP REST API and is disabled by default.
Guest VM support	The TOE appliance can host multiple virtual machines. Support for Guest VMs has not been evaluated.
iDRAC	Provides a local interface to monitor and configure the Dell appliance. This interface is not used for any of the TOE's management functions and is therefore outside the scope of the TSF.
SNMP	SNMP provides an SNMP agent for use by network management tools. This connection is unprotected and is disabled in the evaluated configuration via setting 'Common Criteria Mode'.
Backups using SMB or NFS v4	The product supports SMB or NFS v4 to export system backups to a remote backup server. Backup data is encrypted but SMB and NFS are not approved protocols. SSHFS and SCP (based on SSH) are supported and should be used instead to export backups.
Access control mechanisms (e.g.: rate limiting, policy settings)	Access control mechanisms like rate limiting are outside the scope of the [cPPND] and therefore they have not been evaluated.
High-availability and multi-master database transactions and replication	The TOE includes the TLS protected communication for database channels. The actual database transactions, replication and high-availability functions have not been evaluated since the [cPPND] does not define those functions.
Load balancing	The product implements hooks to integrate with external 3rd party load balancers. The hooks are provided over plain HTTP (not HTTPS) and are disabled when operating in Common Criteria mode.
Any features not associated with SFRs in claimed [cPPND]	[cPPND] forbids adding additional requirements to the Security Target (ST). If additional functionalities or products are mentioned in the ST, it is for completeness only.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Trusted Security Foundation 400, Version 3.2 ([13]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 ([6]). The evaluation determined the TOE satisfies the conformance claims made in the QuintessenceLabs Trusted Security Foundation 400, Version 3.2 Security Target, of Part 2 extended and Part 3 conformant. The TOE satisfies the requirements specified in *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 ([5]).

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team searched the following public vulnerability repositories:

- National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search)
- US-CERT Vulnerability Notes Database (https://www.kb.cert.org/vuls/)
- Tipping Point Zero Day Initiative (https://www.zerodayinitiative.com/advisories/published/)
- OpenSSL vulnerabilities (https://openssl-library.org/news/vulnerabilities-1.1.1/index.html).

The Supporting Document [6] specifies additional sources of vulnerability information, but each source listed there that is not listed here was found to use the National Vulnerability Database (i.e., CVEs) as its input data. Therefore, they do not contain any potential vulnerabilities that were not discovered via review of the materials referenced above.

The searches were completed on 3/10/2025, updated on 4/3/2025, and again updated on 5/14/2025, using search terms that referenced the TOE itself, the processor that the TOE uses, the operating system, the cryptographic library, and the list of additional third-party software components provided by the vendor.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the evaluation activities specified in the claimed PP. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness. All the excluded functionalities are found in section 8.2.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Security Target

The ST for this product's evaluation is QuintessenceLabs Trusted Security Foundation 400, Version 3.2 Security Target, Version 1.0, March 5, 2025 [7].

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
cPP	collaborative Protection Profile
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PCL	Product Compliant List
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

13 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.

[6] Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP, Version 2.2, December 2019.

[7] QuintessenceLabs Trusted Security Foundation 400, Version 3.2 Security Target, Version 1.0, March 5, 2025.

[8] QuintessenceLabs Common Criteria (CC) Evaluated Configuration Guidance, Version 1.0, March 26, 2025

[9] QuintessenceLabs Advanced Administration Guide, TSF KMS 3.2, March 6, 2025

[10] QuintessenceLabs Common Criteria CLI Guide, TSF KMS 3.2, March 14, 2025

[11] QuintessenceLabs Getting Started Guide, TSF KMS 3.2, March 6, 2025

[12] QuintessenceLabs User Guide, TSF KMS 3.2, March 6, 2025

[13] Evaluation Technical Report for Trusted Security Foundation 400, Version 3.2, Version 1.0, April 14, 2025.

[14] Assurance Activities Report for QuintessenceLabs Trusted Security Foundation 400, Version 3.2, Version 1.0, April 14, 2025.

[15] QuintessenceLabs Trusted Security Foundation 400, Version 3.2 Test Report and Procedures for Network Device collaborative PP Version 2.2e, Version 1.0, April 11, 2025.