National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

RedSeal Server v10.5

Report Number: CCEVS-VR-VID11595-2025
Dated: 27 October 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

Jenn Dotson
Randy Heimann
Lisa Mitchell
Linda Morrison
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) Validation team's assessment of the evaluation of RedSeal Inc.'s RedSeal Server v10.5 (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.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in October 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Leidos, Inc. The evaluation determined that the TOE is both 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 3.0E, 6 December 2023 [NDcPP]
- *Functional Package for Secure Shell (SSH),* Version 1.0, 13 May 2021 [SSHPKG].

The TOE is the RedSeal Server v10.5. 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). This VR applies only to the specific version of the TOE as evaluated. 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 and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). The Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *RedSeal Server v10.5 Security Target*, Version 1.0, 17 October 2025, and analysis performed by the Validation team.

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	RedSeal Server v10.5
Security Target	*RedSeal Server v10.5 Security Target*, Version 1.0, 17 October, 2025
Evaluation Technical Report	*Evaluation Technical Report for RedSeal Server v10.5*, Version 1.0, 17 October, 2025
Sponsor & Developer	RedSeal, Inc. 1600 Technology Drive, 4th Floor San Jose CA, 95110
Completion Date	27 October 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 3.0E, 6 December 2023 *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021
Conformance Result	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	Allen Sant, Armin Najafabadi, Greg Beaver, Pascal Patin
Validation Personnel	Jenn Dotson, Randy Heimann, Lisa Mitchell, Linda Morrison, Lori Sarem

3 TOE Architecture

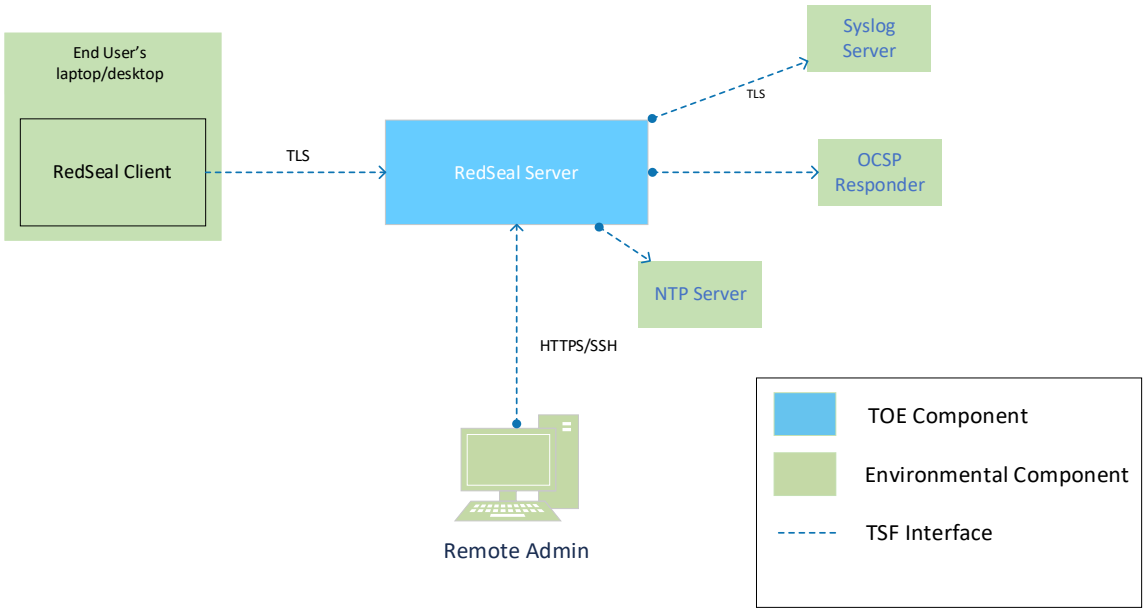
The TOE comprises the RedSeal Server application running on a Linux operating system, together with a database, all installed on a physical appliance provided by RedSeal. The product can be provisioned as a virtual appliance image and deployed on a virtual platform; however, these virtual deployments were not part of the evaluated configuration.

The RedSeal Server application includes the following main server processes:

- Admin server—provides administrative and infrastructure services to several other processes making up the RedSeal application
- RedSeal server—manages the import of network device configurations, contains the analysis engine, and provides the database interface.

The TOE includes a Linux distribution (RHEL 9.6) that provides the operating system on which the RedSeal application executes, and Temurin JRE 17.0.15+6, which supports part of the TOE's cryptographic algorithm implementation. The TOE (through an integrated Dell BSAFE SSL-J v7.3.1) implements cryptographic algorithms that support secure communication: between the TOE's browser-based Web Beta client and the remote administrative users (HTTPS); between the TOE and the Java client (TLS); between the TOE and the audit server (TLS); and between the TOE and legacy web clients (HTTPS). The TOE also includes OpenSSL 3.2.2-6, which provides the cryptographic algorithms to support SSH connections to the CLI.

The figure below shows the TOE in a sample deployment in its operational environment.



4 Security Policy

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

4.1 Security Audit

The TOE generates audit records of security relevant events, including the events specified in [NDcPP] and [SSHPKG]. The TOE stores audit records locally and can also be configured to send the audit records to an external syslog server over a protected communication channel.

The logs comprising the audit trail are stored in the TOE's filesystem and protected from unauthorized modification and deletion by file system permissions. The TOE maintains a maximum of five log files—the current log file and four backups or archives. Each file has a default maximum of 50 megabytes (which is configurable by an administrator). When the current log file reaches its configured maximum size, it is closed and rotated to an archive, and a new current log file is created. If the maximum number of archive files already exists, the oldest one is deleted. The TOE will generate a warning message if the storage space for audit records reaches 75% capacity.

4.2 Cryptographic Support

The TOE implements cryptographic algorithms and mechanisms that provide random bit generation, asymmetric cryptographic key pair generation, key establishment, symmetric data encryption and decryption, digital signature generation and verification, cryptographic hashing, and keyed-hash message authentication services in support of higher-level cryptographic protocols, including SSH and TLS.

4.3 Identification and Authentication

The TOE requires all users to be successfully identified and authenticated prior to accessing its security management functions and other capabilities. The TOE offers only remote access (via SSH) to a CLI (no local access); remote access (via HTTPS) to a browser-based administrative Web Beta client; and remote access (protected by TLS) using the Java client (either as a standalone Java application or the web-based Remote client) to support interactive administrator sessions.

The TOE provides a local password-based authentication mechanism for all users and enforces a minimum length for passwords. SSH public key authentication is also supported for the CLI. The TOE will deny remote access to a user after a configurable number of consecutive failed password authentication attempts (default is three).

4.4 Security Management

The TOE provides the security management functions necessary to configure and administer its security capabilities, including: configuring a login access banner; configuring a remote session inactivity time limit before session termination; configuring the parameters (number of consecutive failures, lockout period) for the authentication failure handling mechanism; setting the system date and time and also configuring NTP; performing software updates and verifying updates using a digital signature.

The TOE provides a CLI to access its security management functions. Administrators can access the CLI remotely using SSH (no local access provided). Additionally, some security management functions are

accessible via the Web Beta client and the Java client. Security management commands are limited to administrators and are available only after they have been successfully identified and authenticated.

4.5 Protection of the TSF

The TOE protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator.

The TOE provides reliable time stamps for its own use and can be configured to synchronize its time via NTP.

The TOE provides a trusted means for determining the current running version of its software and to update its software. The integrity of software updates can be verified using a digital signature.

The TOE implements various self-tests that execute during the power-on and start up sequence, including firmware/software integrity tests and cryptographic known answer tests that verify the correct operation of the TOE's cryptographic functions.

4.6 TOE Access

The TOE will terminate 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 (no local access to CLI provided); TLS using the Java client/Remote client (for remote GUI access to the management interface whether through a standalone thick client or a browser-based Java implementation); and using HTTPS (for accessing the TOE's administrative Web Beta client).

The TOE is able to protect transmission of audit records to an external audit server using TLS.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *collaborative Protection Profile for Network Device*, Version 3.0e, 6 December 2023 [NDcPP]
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [SSHPKG]

That information has not been reproduced here and the NDcPP/SSHPKG should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP/SSHPKG as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the NDcPP with the SSHPKG and performed by the Evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific TOE models was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.
- 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP/SSHPKG and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

RedSeal 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:

- *RedSeal Server v10.5 Common Criteria Evaluated Configuration Guide,* Version 1.0, 24 Oct 2025
- *RedSeal Installation and Administration Guide*, Version 10.5.2

To use the product in the evaluated configuration, the product must be configured as specified in this documentation. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

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.

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:

- *RedSeal Server 10.5 Common Criteria Test Report and Procedures for Network Device collaborative PP Version 3.0e,* Version 1.0, 17 October 2025

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

- *Assurance Activities Report for RedSeal Server v10.5*, Version 1.0, 17 October 2025

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

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 NDcPP and SSHPKG.

The Evaluation team devised a Test Plan based on the test evaluation activities in the materials referenced above. 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 May 2025 to October 2025.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the guidance provided, 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 NDcPP and SSHPKG were fulfilled.

7.3 Test Configuration

The Evaluation team established a test configuration consisting of the TOE (RedSeal Server) appliance deployed in an environment with the following dependencies:

- TLS Test Server: used for TLS client/server testing and port scanning
- Revocation Test Server: used to test X.509 revocation
- NTP Server: used to test NTP time synchronization

Specific test configuration information can be found in the proprietary Test Plan.

8 Evaluated Configuration

The TOE consists of a RedSeal G5C Appliance as defined in the following table, running firmware version 10.5.2.

Height	1.7 in (43 mm)
Width	17.2 in (437 mm)
Depth	23.5 in (597 mm)
Weight	46 lbs (20 kg)
Temperature	50 – 95 degrees F (10 – 35 degrees C)
Humidity (noncondensing)	8 – 90 %
Voltage	100-240V, 8.5A-3.8A, 50-60 Hz
Processor	Intel Xeon Gold 5217 (Cascade Lake)
RAM	256 GB, 2933 MHz
Disk storage	Seagate 2.5”, 1TB, SATA3 6Gb/s, 7.2K RPM, 512N, 128M
Power	Dual hot plug redundant (1 + 1) 700W

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

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 rev 5 and CEM version 3.1 rev 5. The Evaluation team determined the RedSeal Server v10.5 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP/SSHPKG.

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

The Evaluation team performed each TSS assurance activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description (also referred as the TOE Architecture), 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 RedSeal Server v10.5 that are consistent with the claimed Protection Profile, and security function descriptions that satisfy the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The Evaluation team performed each assurance activity and applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the Evaluation team performed the assurance activities specified in the NDcPP/SSHPKG related to the examination of the information contained in the TSS.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team performed each guidance assurance activity and applied each AGD CEM 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.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in

accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each ALC CEM work unit. The Evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

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

The Evaluation team performed each test activity and applied each ATE 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.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed a search of the following online sources:

- National Vulnerability Database (https://nvd.nist.gov/)
- US-Cert (https://www.kb.cert.org/vuls/html/search)
- Tipping Point Zero Day Initiative (https://www.zerodayinitiative.com/advisories/published/)
- RedHat (https://access.redhat.com/security/)
- OpenSSL (https://openssl-library.org/news/vulnerabilities/)

The searches were performed several times, most recently October 15, 2025, using the following search terms:

- RedSeal Server v10.5
- Intel Xeon 5217
- Cascade Lake
- RedHat Enterprise Linux v9.6
- Java Runtime Environment (JRE) Temurin 17.0.15+6
- RedSeal Server v10.5
- OpenSSL 3.2.2-6
- openssh-8.7p1-45
- Dell BSAFE SSL-J v 7.3.1

- Additional proprietary product specific third-party library search terms

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The Evaluation team 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.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. 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 Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in the Guidance documents defined in Section 6. No versions of the TOE and software, either earlier or later, were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

Per NIAP Scheme Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

11 Security Target

The ST for this product's evaluation is *RedSeal Server v10.5 Security. Target*, Version 1.0, 17 October 2025

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PII	Personally Identifiable Information
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
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 Methodology for Information Technology Security*, Version 3.1, Revision 5, April 2017.

[5] *collaborative Protection Profile for Network Devices*, Version 3.0E, 6 December 2023

[6] *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021

[8] *RedSeal Server v10.5 Security Target*, Version 1.0, 17 October 2025

[9] *RedSeal Server v10.5 Common Criteria Evaluated Configuration Guide*, Version 1.0, 24 Oct 2025

[10] *RedSeal Installation and Administration Guide*, Version 10.5.2

[11] *Evaluation Technical Report for RedSeal Server v10.5*, Version 1.0, 17 October 2025

[12] *Assurance Activities Report for RedSeal Server v10.5*, Version 1.0, 17 October 2025

[13] *RedSeal Server 10.5 Common Criteria Test Report and Procedures for Network Device collaborative PP Version 3.0e,* Version 1.0, 17 October 2025

[14] *RedSeal Server v10.5 Vulnerability Assessment*, Version 1.4, 15 October 2025