National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Extreme Networks Fabric Engine Switches v9.1.100

Report Number: CCEVS-VR-VID11656-2026
Dated: June 2, 2026
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

Jerome Myers
Meredith Martinez
The Aerospace Corporation

Common Criteria Testing Laboratory

Reed Eberly
Ryan Hagedorn
Will Micknick
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Extreme Fabric Engine Switches v9.1.100 solution provided by Extreme Networks, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in June 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 (NDcPP30e) with the Functional Package for SSH, Version 1.0, 13 May 2021 (SSH10).

The Target of Evaluation (TOE) is the Extreme Fabric Engine Switches v9.1.100.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory 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 Validation Report 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 and the conclusions of the testing laboratory in the evaluation technical report 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 of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Extreme Networks Fabric Engine Switches v9.1.100 Security Target, version 0.5, May 28, 2026 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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common

Evaluation Methodology (CEM) 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 information technology 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 Validated Products List.

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile 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	Extreme Fabric Engine Switches v9.1.100 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 (NDcPP30e) with the Functional Package for SSH, Version 1.0, 13 May 2021 (SSH10)
ST	Extreme Networks Fabric Engine Switches v9.1.100 Security Target, version 0.5, May 28, 2026
Evaluation Technical Report	Evaluation Technical Report for Extreme Fabric Engine Switches v9.1.100, version 0.2, May 28, 2026
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Extreme Networks, Inc.
Developer	Extreme Networks, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jerome Myers and Meredith Martinez

3 Architectural Information

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

The TOE is the Extreme Networks Fabric Engine Switches v9.1.100. The TOE is a standalone network device that facilitates Data Link Layer data transfer between network nodes connected to its physical ports. TOE consists of a hardware appliance with embedded firmware. The TOE evaluated configuration is one instance of one of those listed models running Fabric Engine 9.1.100.

All TOE appliances are shipped ready for immediate access through a Command Line Interface [CLI], with some basic features enabled by default. However, to ensure secure use, the product must be configured prior to being put into a production environment as specified in the user guidance. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using SSH. All of the remote management interfaces are protected using encryption.

3.1 TOE Description

The TOE links the Mocana v6.5.2f 32-bit libraries for cryptographic operations using non-PAA operations only with the Mocana GCM 64k feature enabled. Each model includes an out of band management port that is Intel-based and a set of in band network interfaces that are all Broadcom-based. Therefore, all models have equivalent network interfaces.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

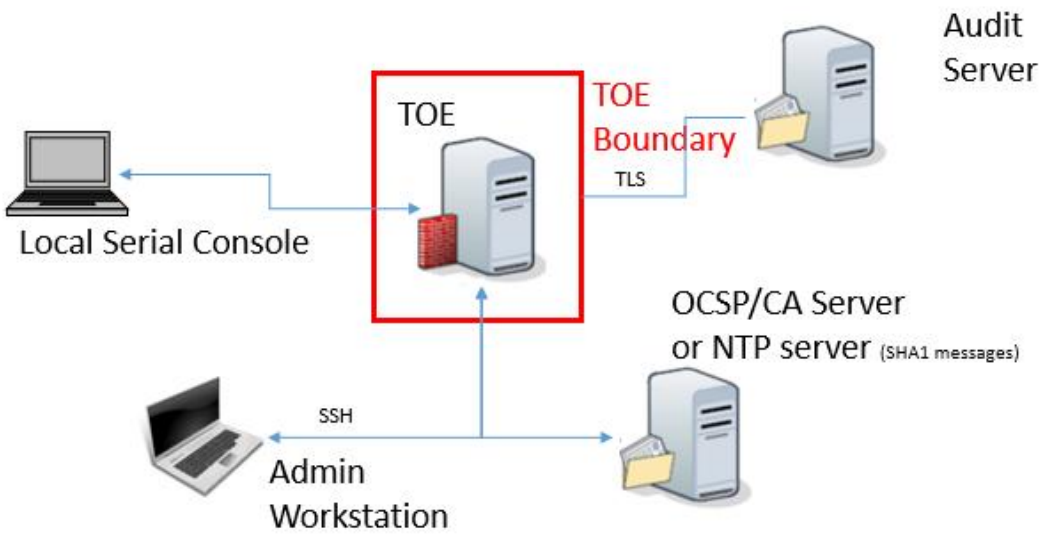
3.3 TOE Architecture

The basic architecture of each TOE appliance begins with a hardware appliance with physical network connections. Within the hardware appliance the TOE is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions).

There are normally two management interfaces – a browser-based management UI accessed via TLS/HTTPS and a CLI accessed locally or via SSH. However, to meet the requirements listed in this Security Target, the browser-based management UI must be disabled as described by guidance. Thus, in the evaluated configuration only the CLI can be used for management.

The TOE Boundary is outlined in the following figure:

Figure 1: TOE Boundary



3.4 Physical Boundaries

The physical boundary of the TOE is the Extreme Networks Fabric Engine Switches running software version 9.1.100, which includes:

- The appliance hardware
- RJ-45/RS-232 management ports
- USB port
- Embedded software/firmware installed on the appliance
- CLI management interface

Each TOE appliance runs a version of the Extreme proprietary OS and has physical network connections to its environment to facilitate routing and switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management. The TOE may be accessed and managed through a management workstation or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an audit server (i.e., a syslog server) that is provided by the environment. This is generally advisable given the limited audit log storage space on the evaluated appliances. The TOE sets its internal clock using administrative commands issued at the CLI interface or can use an NTP server.

The evaluation assumes the Operational Environment of the TOE includes the following:

- The SSH client that is used to access the management interface
- The management workstation that hosts the SSH client
- Syslog server for external storage of audit records
- NTP server for synchronizing system time
- Certificate Authority and OCSP servers to support X.509
- DNS server (optional not depicted in Figure 1)

The scope of the evaluation is limited to the requirements levied upon the TOE in the ST – all other functionality is outside the scope of the evaluation.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The Network Appliances provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: failure on invoking cryptographic functionality such as establishment, termination and failure of a TLS session; establishment, termination and failure of an SSH session; all use of the user identification mechanisms; any use of the authentication mechanism; any change in the configuration of the TOE, changes to time, initiation of TOE update, indication of completion of TSF self-test, termination of a remote session; and initiation and termination of a trusted channel.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using TLS. The logs for all appliances can be viewed the CLI. The records include the date/time the event occurred, the event/type of event, the user ID associated with the event, and additional information of the event and its success and/or failure.

4.2 Cryptographic support

The TOE utilizes CAVP-tested cryptographic implementations to provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols. This cryptography is used to support the following features:

- TLS client in support of secure channel with remote syslog server,
- SSH server in support of secure CLI remote management interface,
- X.509 certificate validation, and
- NTP support.

4.3 Identification and authentication

The TOE provides authentication services for administrative users to connect to the TOEs administrator interfaces (local CLI, and remote CLI). The TOE requires Administrators to authenticate prior to being granted access to any of the management functionality. In the Common Criteria evaluated configuration, the TOE requires a minimum password length be configured between 8 and 32 characters, as well as a minimum RSA key length of 2048 bits. The TOE provides administrator authentication against a local user database.

4.4 Security management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Management can take place over a variety of interfaces including:

- Local console command line administration;
- Remote command line administration via SSHv2;

The TOE provides multiple interfaces to perform administration. While in the CLI command mode, the administrator has access to six distinct modes, or privileges, that provide access to a specific set of commands. Depending on RBAC configuration, not every administrative account would have access to all modes. The CLI modes are as follows:

- User EXEC Mode: Initial mode of access.
- Privileged EXEC Mode: User mode and password combination determines access level.
- Global Configuration Mode: Use this mode to make changes to the running configuration.
- Interface Configuration Mode: Use this mode to modify or configure logical interface, VLAN or a physical interface.
- Router Configuration Mode: Use this mode to modify protocol settings.
- Application Configuration Mode: Use this mode to access the applications.

The system allows administrators to view audit records in EXEC mode.

All administrative functionality is accessed via the CLI. The TOE audits all administrative access. The TOE displays login banners and inactivity timeouts to terminate idle administrative sessions after a set period of inactivity.

4.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls restrictions to management and configuration functionality to Administrators. The TOE prevents reading of private keys and plaintext passwords by any user. The TOE internally maintains the date and time. This date and time are used as a timestamp that is part of each audit record generated by the TOE. Administrators can update the TOE's clock manually or can configure the TOE to synchronize with an external time source. The TOE performs testing to verify correct operation of the security appliances themselves. The TOE verifies all software updates via

digital signature (2048-bit RSA/SHA-256) and requires administrative intervention prior to the software updates being installed on the TOE to avoid the installation of unauthorized firmware.

4.6 TOE access

The TOE can terminate inactive sessions after a configurable period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE can also display specified banner on the local and remote CLI interfaces prior to allowing any administrative access to the TOE. The TOE allows users to manually terminate an established management session with the TOE.

4.7 Trusted path/channels

The TOE supports several types of secure communications:

- Trusted paths with remote administrators over SSH,
- Trusted channels with remote IT environment syslog servers over TLS.

5 Assumptions & 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 Devices, Version 3.0e, 06 December 2023 (NDcPP30e)
- Functional Package for SSH, Version 1.0, 13 May 2021 (SSH10)

That information has not been reproduced here and the NDcPP30e/SSH10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP30e/SSH10 as described for this TOE in the Security Target. 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.

5.2 Clarification of scope

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 collaborative Protection Profile for Network Devices with the SSH Package 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 Guide, additional customer documentation for the specific Network Device models was not included in the scope of the evaluation and therefore should not to 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 NDcPP30e/SSH10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

5.3 TOE Excluded Functionality

The TOE supports a number of features that are not part of the core functionality. These features are not included in the scope of the evaluation:

- Browser-based management UI accessed via TLS/HTTPS is disabled and is not evaluated.
- The use of SNMPv3 is excluded.
- The REST and NETCONF management interfaces are not evaluated.
- Fabric Extend with IPsec is not evaluated.
- Use of the FTP server is excluded and is disabled by default.
- Integration with AAA server is not evaluated.
- Virtualized products are not included in the scope and are not evaluated.

6 Documentation

The following documents were available with the TOE for evaluation:

- Extreme Fabric Engine Common Criteria Configuration Guide 9.1.100, May 2026

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Extreme Fabric Engine Switches v9.1.100, Version 0.2, May 28, 2026 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

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 evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP30e/SSH10 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The TOE consists of the following hardware models:

Table 2: Extreme networking appliances – hardware

Platform	Series	Processor
Fabric Engine 9.1.100	U5320	BCM56175, BCM56274
	U5420	BCM56274, BCM56275
	U5520	BCM56375, BCM56376
	U5720	Intel Atom C3338, C3538
	U7520	Intel Atom C3758
	U7720	Intel Atom C3758

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 determined the Fabric Engine Switches v9.1.100 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP30e/SSH10.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement

of security requirements claimed to be met by the Extreme Fabric Engine Switches v9.1.100 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 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 Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP30e/SSH10 related to the examination of the information contained in the TOE Summary Specification (TSS).

The validator 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 applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator 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 applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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 applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP30e/SSH10 and recorded the results in a Test Report, summarized in the AAR.

The validator 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 (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

On May 28, 2026, the evaluator searched the (National Vulnerability Database (https://web.nvd.nist.gov/vuln/search, ref NVD), MITRE CVE Database, National Vulnerability Database, and CVE details (https://www.cve.org/, https://web.nvd.nist.gov/vuln/search, and https://www.cvedetails.com/vulnerability-search.php, ref CVE), Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog, ref KEV), Vulnerability Notes Database (http://www.kb.cert.org/vuls/, ref VND), Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities, ref Rapid7), Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories, ref ZDI), Tenable Network Security (http://nessus.org/plugins/index.php?view=search, ref TEN), Offensive Security Exploit Database (https://www.exploit-db.com/, ref EDB) with the following search terms: “Extreme”, “VOSS”, “VSP”, “Intel Atom”, “Fabric Engine”, “Extreme Networks”, “Mocana”, “Broadcom”, “DigiCert”.

Further details regarding the vulnerability analysis are found in Section 3.4.2 of the AAR.

The validator 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

All validator comments are covered in other sections of this Validation Report.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Extreme Networks Fabric Engine Switches v9.1.100 Security Target, version 0.5, May 28, 2026*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

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

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

[4] collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 (NDcPP30e).

[5] Functional Package for SSH, Version 1.0, 13 May 2021 (SSH10).

[6] Extreme Networks Fabric Engine Switches v9.1.100 Security Target, version 0.5, May 28, 2026 (ST).

[7] Assurance Activity Report for Extreme Fabric Engine Switches v9.1.100, Version 0.2, May 28, 2026 (AAR).

[8] Detailed Test Report for Extreme Fabric Engine Switches v9.1.100, Version 0.2, May 28, 2026 (DTR).

[9] Evaluation Technical Report for Extreme Fabric Engine Switches v9.1.100, Version 0.2, May 28, 2026 (ETR).