National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Extreme Networks Switching Engine version 33.4.100

Report Number: CCEVS-VR-VID11688-2026
Dated: September 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

Farid Ahmed
Robert Wojcik
Anne Gugel
Lynne Ambuel
Johns Hopkins University Applied Physics Laboratory

Matt Downey
NIAP/CCEVS

Common Criteria Testing Laboratory

Tammy Compton
Cody Cummins
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 Networks Switching Engine version 33.4.100 solution provided by Extreme Networks, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report 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 August 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 Networks Switching Engine version 33.4.100.

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 Switching Engine version 33.4.100 Security Target, version 0.4, August 4, 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 Networks Switching Engine version 33.4.100 (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 Secure Shell (SSH), Version 1.0, 13 May 2021 (SSH10)
ST	Extreme Networks Switching Engine version 33.4.100 Security Target, version 0.4, August 4, 2026
Evaluation Technical Report	Evaluation Technical Report for Extreme Networks Switching Engine version 33.4.100, version 0.2, August 4, 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	Matt Downey, Farid Ahmed, Robert Wojcik, Anne Gugel, and Lynne Ambuel

3 Architectural Information

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

The TOE is the Extreme Networks Switching Engine version 33.4.100. The TOE provides high density layer 2/3 switching with low latency cut-through switching and IPv4 and IPv6 unicast and multicast routing to enable enterprise aggregation and core backbone deployments. The TOE consists of a hardware appliance with embedded software components.

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 TOE guidance.

3.1 TOE Description

The TOE consists of both hardware and software components. The TOE consists of the following series of appliances all running software version 33.4.100:

Platform	Model	Processor
Switching Engine 33.4.100	U5320	Broadcom BCM56175, BCM56274 (ARMv8)
	U5420	Broadcom BCM56274, BCM56275 (ARMv8)
	U5520	Broadcom BCM56375 (ARMv8)
	U5720	Intel Atom C3338, C3538 Denverton
	U7520	Intel Atom C3758 Denverton
	U7720	Intel Atom C3758 Denverton

Each hardware profile provides a defined set of performance characteristics - switching bandwidth, latency, and port density while offering the same level of security features.

Switch Engine 5320 Series:
The ExtremeSwitching 5320 Series are standalone Ethernet switches. The x435 Series offers comprehensive Layer 2 switching, static routing, advanced PoE, role-based policy and comprehensive security services. The 5320 Series is suitable for enterprises looking for Ethernet connectivity in branch/small sites or at the network edge.

The Switch Engine 5320 Series consists of the following switches:

Models	Model Specifications
5320-48T-8XE	ExtremeSwitching 5320 48 10/100/1000BASET FDX/HDX, 8 10G unpopulated SFP+, MACSec capable, internal fixed PSU, fans
5320-48P-8XE	ExtremeSwitching 5320 48 10/100/1000BASET FDX/HDX PoE+, 8 10G unpopulated SFP+, MACSec capable, internal fixed PSU, fans
5320-24T-8XE	ExtremeSwitching 5320 24 10/100/1000BASET FDX/HDX, 8 10G unpopulated SFP+, MACSec capable, internal fixed PSU, fans

Models	Model Specifications
5320-24P-8XE	ExtremeSwitching 5320 24 10/100/1000BASET FDX/HDX PoE+, 8 10G unpopulated SFP+, MACSec capable, internal fixed PSU, fans
5320-16P-4XE	ExtremeSwitching 5320 16 10/100/1000BASET FDX/HDX PoE+, 4 10G unpopulated SFP+, MACSec capable, internal fixed PSU, fans
5320-16P-4XE-DC	ExtremeSwitching 5320 16 10/100/1000BASET FDX/HDX PoE+, 4 10G unpopulated SFP+, MACSec capable, internal fixed DC PSU, fans

5320 Series

Switch Engine 5420 Series:

The ExtremeSwitching 5420 Series is a stackable switch family providing secure Gigabit and multi-Gigabit Ethernet connectivity. The 5420 Series offers routing and switching, high-speed stacking, modular uplink options, advanced PoE, and comprehensive security. This makes the x465 Series suitable for high-end wiring closet and network edge deployments.

The Switch Engine 5420 Series consists of the following switches:

Models	Model Specifications
5420F-24T-4XE	24 x 10/100/1000Base-T ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-24P-4XE	24 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-24S-4XE	24 x 1000Base-X (SFP) ports (unpopulated) - Full / Half-Duplex (autosensing) 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-48T-4XE	48 x 10/100/1000Base-T ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-48P-4XE	48 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports -

Models	Model Specifications
	MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-48P-4XL	48 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable - LRM-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-8W-16P-4XE	8 x 10/100/1000Base-T 802.3bt (90W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 16 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-16W-32P-4XE	16 x 10/100/1000Base-T 802.3bt (90W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 32 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-16MW-32P-4XE	16 x 100M/1G/2.5GBase-T 802.3bt (90W) ports - MACsec-capable 32 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420M-24T-4YE	24 x 10/100/1000Base-T ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 10/25Gb SFP28 uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420M-24W-4YE	24 x 10/100/1000Base-T 802.3bt (90W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 10/25Gb SFP28 uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x

Models	Model Specifications
	USB A ports for management or external USB flash 1 x USB Micro-B console port
5420M-48T-4YE	48 x 10/100/1000Base-T ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 10/25Gb SFP28 uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420M-48W-4YE	48 x 10/100/1000Base-T 802.3bt (90W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 10/25Gb SFP28 uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420M-16MW-32P-4YE	16 x 100M/1G/2.5GBase-T 802.3bt (90W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 32 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 10/25Gb SFP28 uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port

5420 Series

Switch Engine 5520 Series:

The 5520 Series is a family of feature-rich edge and aggregation switches. The 5520 Series universal hardware provides end-to-end secure network segmentation and advanced policy capabilities. The 5520 platform can be deployed across a range of edge, aggregation and wiring-closet environments.

The Switch Engine 5520 Series consists of the following switches:

Models	Model Specifications
5520-24T	5520 Universal Switch with 24 x 10/100/1000BASE-T full/half duplex MACsec-capable ports, includes 2 x Stacking/QSFP28 ports, 2 fan modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-24W	5520 Universal Switch with 24 x 10/100/1000BASE-T full/half duplex 802.3bt 90W PoE MACseccapable ports, includes 2 x Stacking/QSFP28 ports, 3 fan modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-48T	5520 Universal Switch with 48 x 10/100/1000BASE-T full/half duplex MACsec-capable ports, includes 2 x Stacking/QSFP28 ports, 3 fan

Models	Model Specifications
	modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-48W	5520 Universal Switch with 48 x 10/100/1000BASE-T full/half duplex 802.3bt 90W PoE MACsec capable ports, includes 2 x Stacking/QSFP28 ports, 3 fan modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-12MW-36W	5520 Universal Switch with 12 x 100Mb/1Gb/2.5Gb/5Gb 802.3bt 90W PoE MACsec-capable ports plus 36 x 10/100/1000BASE-T 802.3bt 90W PoE full/half duplex MACsec-capable ports, includes 2 x Stacking/QSFP28 ports, 3 fan modules, 1VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-48SE	5520 Universal Switch with 48 x 100M/1Gb SFP MACsec-capable ports, includes 2 x Stacking/ QSFP28 ports, 3 fan modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-24X	5520 Universal Switch with 24 x 100Mb/1Gb/10Gb SFP+ ports, includes 2 Stacking/QSFP28 ports, 2 fan modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription

5520 Series

Switch Engine 5720 Series:
The 5720 Series is a family of feature-rich edge and aggregation switches designed for the next generation digital enterprise. The 5720 Series universal hardware provides end-to-end secure network segmentation and advanced policy capabilities. The 5720 platform can be deployed across a range of edge, aggregation and wiring-closet environments.

The Switch Engine 5720 Series consists of the following switches:

Models	Model Specifications
5720-24MW	24 port 802.3bt 90w PoE Switch, multi-rate up to 5G, MACSEC
5720-48MW	48 port 802.3bt 90w PoE Switch, multi-rate up to 5G, MACSEC
5720-24MXW	24 port 802.3bt 90w PoE Switch, multi-rate up to 10G, MACSEC
5720-48MXW	48 port 802.3bt 90w PoE Switch, multi-rate up to 10G, MACSEC

5720 Series

Switch Engine 7520 Series:
The 7520 Series is a family of feature-rich edge and aggregation switches designed for the next generation digital enterprise. The 7520 Series universal hardware provides end-to-end secure network segmentation and advanced policy capabilities. The 7520 platform can be deployed across a range of edge, aggregation and wiring-closet environments.

The Switch Engine 7520 Series consists of the following switches:

Models	Model Specifications
7520-48XT-6C	7520 – A high-performance, fixed-form switch with 48 × 10GbE SFP+ ports and 6 × 40/100GbE uplinks, designed for data center leaf/spine or high-density aggregation with advanced Layer 2/3 and VXLAN/EVPN support.
7520-48Y-8C	7520 – A high-performance, fixed-form switch with 48 × 25GbE SFP28 ports and 6 × 40/100GbE uplinks, ideal for data center leaf/spine or high-density aggregation with advanced Layer 2/3 and VXLAN/EVPN support.

7520 Series

Switch Engine 7720 Series:
The 7720 Series is a family of feature-rich edge and aggregation switches designed for the next generation digital enterprise. Powered by Extreme Networks ExtremeXOS (EXOS), the 7720 Series universal hardware provides end-to-end secure network segmentation and advanced policy capabilities. The 7720 platform can be deployed across a range of edge, aggregation and wiring-closet environments.

The Switch Engine 7720 Series consists of the following switches:

Models	Model Specifications
7720-32C	7720 – A high-performance, fixed-form switch with 32 × 100GbE QSFP28 ports, delivering up to 6.4 Tbps for data center spine or core deployments with advanced Layer 2/3 and VXLAN/EVPN support.

7720 Series

3.2 TOE Evaluated Platforms

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

3.3 TOE Architecture

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, and processor and software that implements routing and switching functions, configuration information and drivers. While hardware varies between different appliance models, the EXOS software is shared across all platforms.

EXOS is composed of subsystems designed to implement operational, security, management, and networking functions. Hardware-specific device drivers that reside in the kernel provide abstraction of the hardware components. A dedicated cryptographic module is integrated with protocol libraries that implement secure channel functionality. A control plane subsystem that includes Internet Protocol (IP) host stack, which can be further subdivided into protocol and control layers, implements switching and routing functions. A system management subsystem, that includes an Authentication, Authorization and Accounting (AAA) module, implements an administrative interface and maintains configuration information.

The figure below outlines the TOE Architecture:

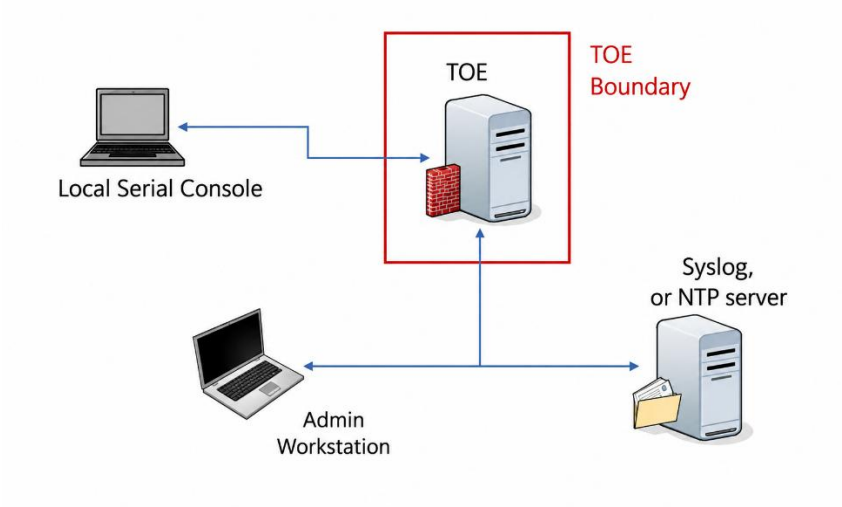

Figure 1 TOE Operational Environment

3.4 Physical Boundaries

The physical boundary of the TOE is Extreme Networks Switching Engine version 33.4.100. EXOS is based on Linux Kernel version 5.10.177.

The Operational Environment of the TOE includes:

- The SSH client that is used to access the management interface
- The management workstation that hosts the SSH client
- Audit server for external storage of audit records
- NTP server for synchronizing system time
- Certificate Authority and OCSP servers to support X.509

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 TOE generates audit records for all security-relevant events. For each audited event, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event. The resulting records are stored locally and can be sent securely to a designated audit server for archiving. Security Administrators, using the appropriate CLI commands, can also view audit records locally. The TOE provides a reliable timestamp relying on the appliance's built-in clock or using an NTP server.

4.2 Cryptographic support

The TOE performs the following cryptographic functionality:

- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification utilizing a dedicated cryptographic library
- Cryptographic functionality is utilized to implement secure channels
  - SSHv2
  - TLS v1.2
- Entropy is collected and used to support seeding with full entropy
- Critical Security Parameters (CSPs) internally stored and cleared when no longer in use
- X509 Certificate authentication integrated with TLS protocol.

The TOE uses a dedicated cryptographic module to manage CSPs and implements deletion procedures to mitigate the possibility of disclosure or modification of CSPs. Additionally, the TOE provides commands to on-demand clear CSPs (e.g. host RSA keys), that can be invoked by a Security Administrator with appropriate permissions.

4.3 Identification and authentication

The TOE supports Role-Based Access Control (RBAC) managed by an Authentication, Authorization, and Accounting (AAA) module (AAA server integration is not evaluated) that stores and manages permissions of all users and their roles. The TOE requires users to provide their assigned unique username and password before any administrative access to the system is granted. Alternatively, the TOE can be configured to rely on an external Radius server for authentication.

Each authorized user is associated with an assigned role and role-specific permissions that determine their access to TOE features. The AAA module stores the assigned role of each user along with all other information required for that user to access the TOE. All TOE management functions are restricted to the Security Administrator.

The TOE supports X509v3 certificate validation during negotiation of TLS protected syslog, TLS protected Radius, and SSH X509 authentication. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE.

4.4 Security management

The TOE allows remote administration using an SSHv2 session, and local administration using a console. Both remote and local administration are conducted over a Command Line Interface (CLI) terminal that facilitates access to all of the management functions used to administer the TOE.

There are two types of administrative users within the system: Security Administrator and User. All of the management functions are restricted to Security Administrators, including: managing user accounts and roles, rebooting and applying software updates, administering the system configuration, and reviewing audit records. The term "Security Administrator" is used to refer to any administrative user with the appropriate role to perform the relevant functions.

4.5 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features.

- The TOE protects CSPs, including stored passwords and cryptographic keys, so they are not directly viewable or accessible in plaintext.
- The TOE ensures that reliable time information is available for both log accountability and synchronization with the operating environment.
- The TOE performs self-tests to detect internal failures and protect itself from malicious updates.

4.6 TOE access

The TOE will display a customizable banner when an administrator initiates an interactive local or remote session. The TOE also enforces an administrator-defined inactivity timeout after which any inactive session is automatically terminated. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

4.7 Trusted path/channels

The TOE protects remote sessions by establishing a trusted path secured using SSH between itself and the administrator. The TOE prevents disclosure or modification of audit records by establishing a trusted channel using TLS between itself and the audit server. Mutual authentication using client-side x.509v3 certificates is supported by the TOE's TLS client for syslog 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:

- The use of SNMPv3 is excluded.
- Use of the FTP server is excluded and it 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 Switch Engine Common Criteria Configuration Guide, 33.4.100, August 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 Networks Switching Engine version 33.4.100, Version 0.2, August 4, 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 series of appliances all running software version 33.4.100:

Platform	Model	Processor
Switching Engine 33.4.100	U5320	Broadcom BCM56175, BCM56274 (ARMv8)
	U5420	Broadcom BCM56274, BCM56275 (ARMv8)
	U5520	Broadcom BCM56375 (ARMv8)
	U5720	Intel Atom C3338, C3538 Denverton
	U7520	Intel Atom C3758 Denverton
	U7720	Intel Atom C3758 Denverton

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 Extreme Networks Switching Engine version 33.4.100 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 Networks Switching Engine version 33.4.100 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 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.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “Extreme”, “EXOS”, “XOS”, “TLS”, “SSH”, “Intel Atom”, “Cavium Octeon”, “BCM53549”, “BCM56375”, “BCM56376”, “BCM56377”, “BCM53547”, “BCM53548”, and ”Broadcom”.

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

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Extreme Switch Engine Common Criteria Configuration Guide, 33.4.100 Supporting Series 7720, 7520, 5520, 5420, 5320, 4220, 4120 August 2026 document. 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 Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server and other network infrastructure, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Extreme Networks Switching Engine version 33.4.100 Security Target, Version 0.4, August 4, 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 Secure Shell (SSH), Version 1.0, 13 May 2021 (SSH10).

[6] Extreme Networks Switching Engine version 33.4.100 Security Target, Version 0.4, August 4, 2026 (ST).

[7] Assurance Activity Report for Extreme Networks Switching Engine version 33.4.100, Version 0.2, August 4, 2026 (AAR).

[8] Detailed Test Report for Extreme Networks Switching Engine version 33.4.100, Version 0.2, August 4, 2026 (DTR).

[9] Evaluation Technical Report for Extreme Networks Switching Engine version 33.4.100, Version 0.2, August 4, 2026 (ETR).