National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Gigamon GigaVUE Fabric Manager v6.6

Report Number: CCEVS-VR-VID11504-2025
Version 1.0
Date: January 31, 2025

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, Senior Validator - Aerospace Corporation
Swapna Katikaneni, Lead Validator - Aerospace Corporation

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Evan Seiz
Rachel Kovach

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Gigamon GigaVUE Fabric Manager version 6.6 provided by Gigamon 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 Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in January 2025. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *collaborative Protection Profile for Network Devices Version 2.2e* (NDcPP).

The Gigamon GigaVUE Fabric Manager Version 6.6 is a network device that includes hardware and software. The Gigamon GigaVUE Fabric Manager 's primary functionality is to offer a central location for the configuration, management, and operation of the Gigamon Deep Observability Pipeline which provides network visibility across physical, virtual, and cloud infrastructure. Gigamon-FM allows for the configuring traffic policies, visualizing network topology connectivity, and identifying visibility hot spots within a network.

The Gigamon GigaVUE Fabric Manager Version 6.6 can fulfill the NDcPP2E security requirements by itself. Therefore, the evaluated configuration consists of the TOE as a standalone device and is not deployed in a distributed manner.

The 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), as interpreted by the Assurance Activities contained in the NDcPP. 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 is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the NDcPP Assurance Activities. 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 *Gigamon GigaVUE Fabric Manager v6.6 Security Target v1.0*, dated December 28, 2024, and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Product Compliant 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	Gigamon GigaVUE Fabric Manager v6.6
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	Gigamon GigaVUE Fabric Manager v6.6 Security Target v1.0, dated December 28, 2024
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Gigamon GigaVUE Fabric Manager v6.6" Evaluation Technical Report v1.0 dated January 6, 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Gigamon Inc.
Developer	Gigamon Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Jerome Myers, Senior Validator - Aerospace Corporation Swapna Katikaneni, Lead Validator - Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that the TOE is deployed in a physically secured operational environment and not subjected to any physical attacks.
- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- The TOE is not responsible for protecting network traffic that is transmitted across its interfaces that is not related to any TOE management functionality or generated data.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that regular software and firmware updates will be applied by a TOE Administrator when made available by the product vendor.
- Administrator credentials are assumed to be secured from unauthorized disclosure.
- TOE Administrators are trusted to ensure that there is no unauthorized access possible for sensitive residual information on the TOE when it is removed from its operational environment.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.UNAUTHORIZED_ADMINISTRATOR_ACCESS** – Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
- **T.WEAK_CRYPTOGRAPHY –** Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
- **T.UNTRUSTED_COMMUNICATION_CHANNELS** – Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
- **T.WEAK_AUTHENTICATION_ENDPOINTS –** Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical

network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

- **T.UPDATE_COMPROMISE –** Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
- **T.UNDETECTED_ACTIVITY** – Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
- **T.SECURITY_FUNCTIONALITY_COMPROMISE –** Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
- **T.PASSWORD_CRACKING –** Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
- **T.SECURITY_FUNCTIONALITY_FAILURE –** An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional 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 level of assurance for this evaluation is defined within the *collaborative Protection Profile for Network Devices, Version 2.2e* 27 March 2020, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to security functionality 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 Security Target. All other functionality provided by the device, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, the Gigamon GigaVUE Fabric Manager's configuration, management, and operation of the Gigamon Deep Observability Pipeline capabilities described in Section

1.3 of the Security Target were not assessed as part of this evaluation. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

The evaluated configuration of the TOE is the Gigamon GigaVUE Fabric Manager appliance described in Table 1 running software Version 6.6. In the evaluated configuration, the TOE uses SSH and HTTPS to secure remote command-line administration, and TLS and HTTPS to secure transmissions of security-relevant data from the TOE to external entities such as an audit server and Gigamon GigaVUE (VID11487). The TOE includes administrative guidance in order to instruct Security Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

4 Architectural Information

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

4.1 TOE Introduction

The TOE is a network device as defined in the NDcPP which states: "This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a Network Device (ND). A network device in the context of this cPP is a device connected to the network and has an infrastructure within the network". The TOE consists of the Gigamon GigaVUE Fabric Manager appliance, running software Version 6.6. Thus, the TOE is a network device composed of hardware and software.

4.2 Physical Boundary

The TOE is comprised of both software and hardware. The hardware is comprised of the following:

Table 2 – Hardware Properties

Property	Gigamon-FM
Model/Part Number	GFM-HW1-FM010
Size	One rack unit (1RU)
Processor	Dual Intel Xeon Silver 4110 2.1GHz, 8C/16T
Management	IPMI 2.0 compliant 2 x 1/10G SFP+ 2 x 100/1000M Base-T LAN Serial console (115,200 baud)
Connectors	Back: 4 x 10/100/1000Mbps LOM 1 x 10/100/1000Mbps iDRAC9 Enterprise 1 x DB9 serial 1 x USB 3.0, one USB 2.0 1 x DB15 VGA Front: 2 x USB 2.0 (disabled in BIOS) 1 x DB15 VGA

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 3 – IT Environment Components

Component	Definition
Certification Authority (CA)	A server that acts as a trusted issuer of digital certificates and distributes a CRL that identifies revoked certificates.
Management Workstation	Any general-purpose computer that is used by a Security Administrator to manage the TOE. The TOE can be managed remotely, in which case the

	management workstation requires an SSH client to access the CLI or a web browser to access the Web GUI. The TOE can also be managed locally, in which case the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications.
Audit Server	The audit server connects to the TOE and allows the TOE to send syslog messages to it for remote storage. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
Gigamon GigaVUE Appliances	The Gigamon GigaVUE appliances are separately evaluated products (VID11487) that Gigamon-FM can manage over a secure channel.

5 Security Policy

5.1.1 Security Audit

Audit records are generated for various types of management activities and events. The audit records include the date and time stamp of the event, the event type and subject identity. In the evaluated configuration, the TSF is configured to transmit audit data to a remote audit server using TLS. Audit data is also stored locally to ensure availability of the data if communications with the audit server become unavailable.

5.1.2 Cryptographic Support

The TOE uses sufficient security measures to protect its data in transmission by implementing cryptographic methods and trusted channels. The TOE uses:

- SSH to secure the remote CLI.
- HTTPS to secure the connection to the Web GUI and to the GigaVUE appliances.
- TLS to secure the connection to the audit server.

Cryptographic keys are generated using the Hash_DRBG provided by this module. The TOE destroys plaintext and private keys in both volatile and non-volatile storage.

The following table contains the CAVP algorithm certificates:

Table 4 – Cryptographic Algorithm Table

SFR	Algorithm	CAVP Cert. #
FCS_CKM.1 - ECC key generation schemes	ECDSA KeyGen (FIPS186-4) P-256, P-384, and P-521 ECDSA KeyVer (FIPS186-4) P-256, P-384, and P-521	A6377
FCS_CKM.2 – ECDSA key establishment	KAS-ECC-SSC Sp800-56Ar3 P-256, P-384, and P-521	A6377
FCS_COP.1/DataEncryption	AES CBC 128 bits and 256 bits AES CTR 128 bits and 256 bits AES GCM 128 bits and 256 bits	A6377
FCS_COP.1/Hash	SHA-256, SHA-384, and SHA-512	A6377
FCS_COP.1/KeyedHash	HMAC-256, HMAC-384, and HMAC-512	A6377
FCS_COP.1/SigGen - ECDSA	ECDSA SigGen (FIPS186-4) P-256, P-384, and P-521 ECDSA SigVer (FIPS186-4) P-256, P-384, and P-521	A6377
FCS_RBG_EXT.1	Hash DRBG	A6377

5.1.3 Identification and Authentication

All users must be identified and authenticated to the TOE before being allowed to perform any actions on the TOE, except viewing a warning banner. The TOE provides a local CLI, a remote CLI via SSH, and a Web GUI via HTTPS for administration. Users authenticate to the TOE using one of the following methods:

- Username/password (all user interfaces)
- Username/public key (remote CLI only)

The TSF provides a configurable number of maximum consecutive authentication failures that are permitted by a user. Once this number has been met, the account is locked until a manual unlock

occurs for Web GUI users or an administratively set time for CLI users. Passwords that are maintained by the TSF can be composed of upper case, lower case, numbers and special characters. The Security Administrator can define the minimum password length between 8 and 64 characters. Password information is never revealed during the authentication process including during login failures.

As part of establishing trusted remote communications, the TOE provides X.509 certificate validation functionality. In addition to verifying the validity of certificates, the TSF can check their revocation status using a certificate revocation list (CRL).

5.1.4 Security Management

The TOE has two roles to fulfill the role of Security Administrator: Admin and Super Admin. The Admin is the administrative role for the local CLI and remote CLI. The Super Admin is the administrative role for the Web GUI. Management functions can be performed using the local CLI, remote CLI, and Web GUI. Both Security Administrator roles are able to perform all security-relevant management functionality (such as user management, password policy configuration, application of software updates, and configuration of cryptographic settings) available to their respective interface. All software updates to the TOE can only be performed manually by an Admin role user.

5.1.5 Protection of the TSF

The TOE stores the hashed representation of passwords using SHA-512. The TOE has a hardware clock that is used for keeping time. The time can be manually set by the Security Administrator. The TOE executes a suite of self-tests during boot and at the request of a Security Administrator.

The version of the TOE (both the currently executing version and the latest installed/updated version) can be obtained by an Admin role user from the CLI interface. The updated image is verified through manually validating the correct published hash.

5.1.6 TOE Access

The TOE can terminate inactive local CLI, remote CLI, or Web GUI sessions after a specified time period. Users can also terminate their own interactive sessions on all interfaces. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session. The TOE displays an administratively configured banner on the local CLI, remote CLI, and Web GUI prior to allowing any administrative access to the TOE.

5.1.7 Trusted Path/Channels

The TOE connects and sends data to IT entities that reside in the Operational Environment via trusted channels. In the evaluated configuration, the TOE connects to an audit server using TLS to encrypt the audit data that traverses the channel and connects to the GigaVUE appliances using HTTPS. When accessing the TOE remotely, Security Administrators interface with the TSF using the remote CLI via SSH and the Web GUI via HTTPS.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- Gigamon GigaVUE Fabric Manager v6.6 Supplemental Administrative Guidance for Common Criteria- v1.0
- GigaVUE Administration Guide, Product Version 6.6, Document Version 1.1
- GigaVUE-FM Hardware Appliances Guide, GigaVUE-FM, Product Version 6.6, Document Version 1.1
- GigaVUE-FM Installation and Upgrade Guide Version 6.6, Document Version 1.1

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 device as evaluated.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Gigamon GigaVUE Fabric Manager appliance, running the software v6.6. Section 4.2 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to communicate with the following environment components:

- Certificate Authority (CA) for distribution of certificates and CRLs
- Management Workstation for local and remote administration
- Audit Server for remote storage of audit records
- Gigamon GigaVUE appliances (separate product).

To use the product in the evaluated configuration, the product must be configured as specified in the *Gigamon GigaVUE Fabric Manager v6.6 Supplemental Administrative Guidance for Common Criteria Version 1.0* document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Assurance Activity Report for a Target of Evaluation "Gigamon GigaVUE Fabric Manager v6.6" Assurance Activities Report v1.0,* dated January 6, 2025.

8.1 Test Configuration

The evaluation team configured the TOE for testing according to the *Gigamon GigaVUE Fabric Manager v6.6 Supplemental Administrative Guidance for Common Criteria Version 1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The evaluation team conducted testing in the Booz Allen CCTL facility on an isolated network. Testing was performed against all two management interfaces defined in the ST (local CLI, remote CLI).

No NTP is claimed. Therefore, all platform clocks were set manually by the evaluator using a cell phone as the definitive time source. The TOE was configured to communicate with the following environment components:

- Function: CRL Distribution Point, Certification Authority for Gigamon-FM to GigaVUE appliance connection
  - Linux gigamon2024-pki 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64 GNU/Linux
  - Protocols: HTTP
  - Tools:
    - tcpdump version 4.99.0
    - Certificate Authority/CRL Distribution Point (OpenSSL 1.1.1k)

- Function: CRL Distribution Point, Certification Authority for Gigamon-FM to audit server connection
  - Linux gigamonFM-pki 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64 GNU/Linux
  - Protocols: HTTP
  - Tools:
    - tcpdump version 4.99.0
    - Certificate Authority/CRL Distribution Point (OpenSSL 1.1.1k)

- Function: Syslog Server
  - Linux gigamon2024-syslog 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64 GNU/Linux
  - Protocols: TLS
  - Tools:
    - tcpdump version 4.99.0
    - rsyslogd 8.2102.0 (aka 2021.02)

- Function: GigaVUE HC1
  - GigaVUE-OS 6.5 Rocky Linux 8.7
  - Protocols: HTTPS

- Function: GigaVUE TA200
  - GigaVUE-OS 6.5 Rocky Linux 8.7
  - Protocols: HTTPS

- Function: Switch
  - Model: Cisco Catalyst WS-C Switch, WS-C3560X-24P
  - OS: Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 12.2(55)SE3
  - Protocols: N/A

- Function: Switch
  - Model: Cisco Catalyst WS-C Switch, WS-C2960-24TT-L
  - OS: Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(50)SE4
  - Protocols: N/A

The following machines were used as the Management Workstations ("Test Workstation") for local and remote administration:

- Function: 3 x Administrator Test Workstation
  - Platform: Dell Precision M4800 Laptop/
  - OS: Windows 10 Version 21H2
  - Protocols: TLS, SSH
  - Tools:
    - Wireshark: version 3.6.7, 4.0.7
    - PuTTY .73

- Function: CATL Test Workstation
  - Platform: VMware ESXi based Virtual Machine
  - OS: (Kali GNU/Linux Rolling 2018.3 Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) x86_64 GNU/Linux
  - Protocols: TLS, SSH
  - Tools:
    - Wireshark version 3.6.7
    - PuTTY version 0.73
    - Metasploit 5.0.20-dev
    - John the ripper 1.9.0
    - Nmap version 7.94
    - OpenSSL 1.1.1k

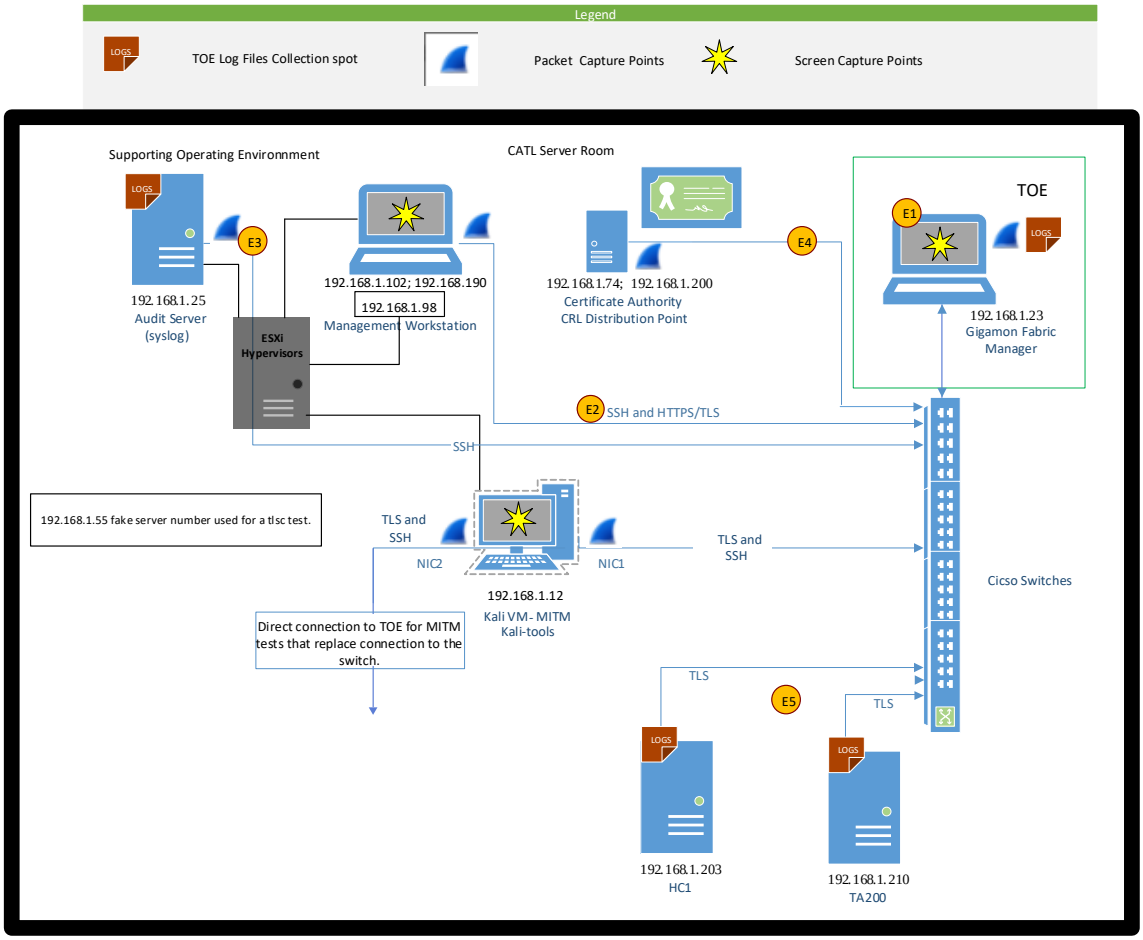

Figure 1 - Test Configuration

8.2 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with NDcPP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords (version information used for refining results) were identified:

Keyword	Description
Gigamon	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
Gigamon-FM	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
GigaVUE-FM	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
Fabric Manager	This is a generic term for searching for known vulnerabilities for the specific product.
Rocky Linux 8.10	This is a generic term searching for known vulnerabilities for the underlying operating system.
Libraries	
See Proprietary List	Provided as a separate proprietary spreadsheet and not reproduced here.
Hardware	
Intel Xeon Silver 4110 (Skylake)	This is a generic term searching for known vulnerabilities for the TOE's underlying host processor.

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources on January 6, 2025. The following public vulnerability sources were searched:

- NIST National Vulnerabilities: https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security http://nessus.org/plugins/index.php?view=search
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test enumerates network port and service information to determine if any ports were open and running services outside of the TOE standard configuration.
- SSH Timing Attack (User Enumeration)

This attack attempts to enumerate validate usernames for the SSH interface, by observing the difference in server response times to valid username login attempts.

- Force SSHv1
  This attack determines if the client will accept both SSHv1 and SSHv2 connections when the TOE claims to only support SSHv2
- CLI Privilege Escalation
  This attack involves enumerating a valid username with an attempt to access the underlying OS CLI shell, then cracking the user's password and logging in.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

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 Evaluation 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 TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

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 Gigamon GigaVUE product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the NDcPP Supporting Documents in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validators 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's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents related to the examination of the information contained in the TOE Summary Specification.

The validators 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 Assurance Activities, 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Document related to the examination of the information contained in the operational guidance documents.

The validators 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 Assurance Activities, 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 units. The evaluation team found that the TOE was identified.

The validators 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 NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validators reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP Supporting Documents, 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 evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validators 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 addressed the vulnerability analysis requirements in the NDcPP Supporting Documents, 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 test activities 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 performed the Evaluation Activities in the NDcPP Supporting Document, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Gigamon GigaVUE Fabric Manager v6.6 Supplemental Administrative Guidance for Common Criteria Version 1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that when the product is configured to offload audit data to an audit server, if that communications link is interrupted, the audit data generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit logs generated during the outage. It will be necessary for the administrator to take steps to offload those logs or they will be overwritten when the audit log is full.

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, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Gigamon GigaVUE Fabric Manager v6.6 Security Target v1.0,* dated December 28, 2024.

13 List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certificate Authority
CAVP	Cryptographic Algorithm Verification Program
CBC	Cipher Block Chaining
CC	Common Criteria
CLI	Command-Line Interface
cPP	collaborative Protection Profile
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSP	Cryptographic Service ProviderIDS
CTR	Counter
DRBG	Deterministic Random Bit Generator
FM	Fabric Manager
FTP	File Transfer Protocol
GMC	Galois/Counter Mode
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
I&A	Identity and Access
IDS	Intrusion Detection System
MAC	Message Authentication Code
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OS	Operating System
PP	Protection Profile
RAM	Random Access Memory
RBG	Random Bit Generator
RNG	Random Number Generator
RU	Rack Unit
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

14 Terminology

Term	Definition
Admin	A user who is assigned the "Admin" role on the TOE's CLI and has the ability to manage the TSF. Synonymous with Security Administrator.
Local CLI	Synonymous with the term "local console".
Super Admin	A user who is assigned the "Super Admin" role on the TOE's Web GUI and has the ability to manage the TSF. Synonymous with Security Administrator.
Credential	Data that establishes the identity of a user (e.g., a cryptographic key or password).
Operating System (OS)	Software that manages hardware resources and provides services for applications.
Platform	A platform can be an operating system, hardware environment, a software-based execution environment, or some combination of these. These types of platforms may also run atop other platforms.
Security Administrator	An authorized administrator role that is authorized to manage the TOE and its data. This TOE defines three separate user roles, but only the most privileged role (Admin) is authorized to manage the TOE's security functionality and is therefore considered to be the Security Administrator for the TOE.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application a Security Administrator uses to manage it (SSH client, terminal client, etc.).
User	In a CC context, any individual who has the ability to access the TOE functions or data.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-001
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-002
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-003
4. Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-004
5. collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020
6. Gigamon GigaVUE Fabric Manager v6.6 Security Target v1.0, dated December 28, 2024
7. Gigamon GigaVUE Fabric Manager v6.6 Supplemental Administrative Guidance for Common Criteria- v1.0
8. GigaVUE Administration Guide, Product Version 6.6, Document Version 1.1
9. GigaVUE-FM Hardware Appliances Guide, GigaVUE-FM, Product Version 6.6, Document Version 1.1
10. GigaVUE-FM Installation and Upgrade Guide Version 6.6, Document Version 1.1
11. Assurance Activity Report for a Target of Evaluation “Gigamon GigaVUE Fabric Manager v6.6” Assurance Activities Report v1.0 dated January 6, 2025