National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3

Report Number: CCEVS-VR-VID11556-2025

Dated: May 30, 2025

Version: 1.0

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

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

ACKNOWLEDGMENTS

Validation Team

Daniel Faigin, Senior Validator

Patrick Mallett, Lead Validator

The Aerospace Corporation

Russ Fink, Lead in Training

Michael Smeltzer, ECR Team

Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Alexander Fannin

Joan Marshall

Acumen Security, LLC

Table of Contents

1 Executive Summary

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

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in May 2025. The information in this report is largely derived from the Security Target (ST) and associated test report. The evaluation determined that the product is 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 and Functional Package for SSH, Version 1.0, 13 May 2021.

The TOE identified in this VR 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 Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional and assurance requirements stated in the ST. Based on these findings, 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 are consistent with the evidence produced.

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). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (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 IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

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(s) 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	Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3
Protection Profile	• collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] • Functional Package for SSH, Version 1.0, 13 May 2021 [PKG_SSH_v1.0]
Security Target	Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3 Security Target, v1.1, 16 May 2025
Evaluation Technical Report	Evaluation Technical Report for KlasOS Keel 5.4.3, v1.5, 16 May 2025
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Klas
Developer	Klas
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Patrick Mallett Daniel Faigin Russ Fink Michael Smeltzer

3 Architectural Information

The TOE is KlasOS Keel (herein referred to as the TOE). It runs the 5.4.3 firmware combining both connectivity and local compute capabilities. This provides users with cloud connectivity when necessary and local processing power for analytics when there is no backhaul. Administration can be performed locally or over a trusted SSH channel.

3.1 TOE Architecture

The following diagram represents the system architecture for the TOE.

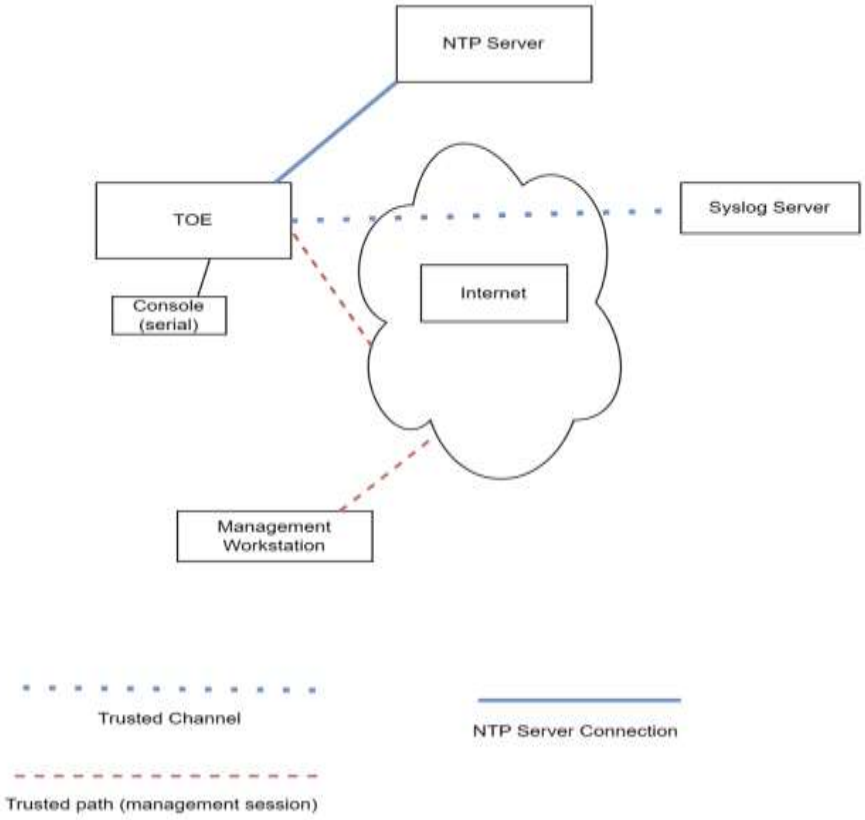

Figure 1 - TOE System Architecture

3.2 Physical Boundaries

The TOE boundary is the hardware appliance which is comprised of hardware and the KlasOS Keel software component. The TOE hardware model is provided in **Table 6 – TOE Model**.

The TOE also supports secure connectivity with several other IT environment devices, including the ones identified in the following table.

The TOE implements SSHv2 to protect the remote management interface for administrators.

Other components are indicated in **Table 2 - TOE Physical Boundary Components**.

Table 2 - TOE Physical Boundary Components

Component	Required	Purpose/Description
Management Workstation	Yes	A management workstation that is directly connected to the TOE's console port may be used by the TOE administrator to support TOE administration. Note: Either a remote or local management workstation, or both can be used.
Remote (Management) Workstation / Remote SSH CLI	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channel. Any SSH client that supports SSHv2 may be used. Note: Either a remote or local management workstation, or both can be used.
Syslog Server	Yes	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. An SSH tunnel is established by the TOE and logs are transmitted using this encrypted method.
NTP Server	No	The NTP server is used to send reliable timestamps to the TOE using NTPv3 and SHA1 as the message digest algorithm.

4 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v3.0e or NDcPP. In addition, the TOE provides security functions for the PP-Configuration for Network Devices. The TOE implements the following security requirements:

- Security Audit (FAU)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of the TSF (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

4.1 Security Audit

The TOE generates audit events for all start-up and shutdown functions as well as all auditable events specified in Table 12 – Security Functional Requirements and Auditable Events [ST]. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE stores audit records locally and will export them to an external syslog server using SSHv2 as a tunnel. Each audit record contains the date and time of the event, type of event, subject identity, and other relevant data for the event. Only a security administrator can enable logging to a syslog server.

4.2 Cryptographic Support

The cryptographic used in the TOE are presented in the following table.

Table 3 –TOE Cryptography Implementation

Cryptographic Methods	Usage
FCS_CKM.1 Cryptographic Key Generation	• Cryptographic key generation conforming to FIPS PUB 186-4 “Digital Signature Standard (DSS)”, Appendix B.3. • RSA Key sizes supported are 2048, 3072 and 4096 bits. • Cryptographic key generation conforming to FIPS PUB 186-4 “Digital Signature Standard (DSS)”, Appendix B.4. • Elliptic NIST curves supported are: P-256, P-384, and P-521.

Cryptographic Methods	Usage
FCS_CKM.2 Cryptographic Key Establishment	• Elliptical curve-based establishment conforming to NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"
FCS_CKM.4 Cryptographic Key Destruction	• Refer to ST v1.1 Table 17 – Cryptographic Key Destruction for Key Zeroization details.
FCS_COP.1/DataEncryption Cryptographic Operations (AES Data Encryption/Decryption)	• AES encryption and decryption conforming to CBC and CTR as specified in ISO 10116. • AES key size supported is 128 and 256 bits • AES mode supported is CBC and CTR
FCS_COP.1/Hash Cryptographic Operations (Hash Algorithm)	• Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. • Hashing algorithms supported are: SHA-1, SHA-256, SHA-384, and SHA-512. • Message digest sizes supported are: 160, 256, 384, and 512 bits.
FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)	• Keyed-hash message authentication conforming to ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm2". • Keyed hash algorithm supported are: HMAC-SHA1, HMAC-SHA-256, HMAC-SHA384, and HMAC-SHA-512 • Key sizes supported are: 160, 256, 384 and 512 bits. • Message digest sizes supported are: 160, 256, 384, and 512 bits.
FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)	• RSA digital signature algorithm conforming to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5;

Cryptographic Methods	Usage
	ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3. • RSA key sizes supported are: 2048, 3072 and 4096 bits. • Elliptical curve digital signature algorithm conforming to FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing NIST curves ISO/IEC 14888-3, Section 6.4. • Elliptical curve key sizes supported are 256 and 384 bits.
FCS_NTP_EXT.1 NTP Protocol	• The TOE supports NTP v3 and adheres to RFC 1305. • Authentication is performed using SHA-1 as the message digest algorithm.
FCS_RBG_EXT.1 Random Bit Generation	• Random number generation conforming to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions” • The TOE leverages CTR_DRBG(AES) • CTR_DRBG seeded with a minimum of 256 bits of entropy.
FCS_SSHS_EXT.1 SSH Server Protocol	• The TOE supports SSH v2 protocol compliant to the following RFCs:4251, 4252, 4253, 4254, 5656, and 6668. • The TOE supports password-based and public-key-based authentication. • SSH public-key authentication uses ssh-rsa, ecdsa-sha2-nistp256 and ecdsa-sha2-nistp384. • SSH transport uses the following encryption algorithms: aes128-cbc, and aes256-cbc. • Packets greater than 262,155 bytes in an SSH transport connection are dropped.

Cryptographic Methods	Usage
	• SSH transport uses the following data integrity MAC algorithms: hmac-sha2-256 and hmac-sha2-512 • Key exchange algorithms supported are: ecdh-sha2-nistp256 and ecdh-sha2-nistp384. • The TOE ensures that during SSH connections, the same session keys are used for a threshold of no longer than one hour and no more than one gigabyte of transmitted data.
FCS_SSHC_EXT.1 SSH Client Protocol	• The TOE supports SSH v2 protocol compliant to the following RFCs:4251, 4252, 4253, 4254, 5656, and 6668. • The TOE supports public-key-based authentication. • SSH public-key authentication uses ssh-rsa, ecdsa-sha2-nistp256 and ecdsa-sha2-nistp384. • SSH transport uses the following encryption algorithms: aes128-cbc, aes 128-ctr, aes128-cbc and aes256-ctr. • Packets greater than 33,292 bytes in an SSH transport connection are dropped. • SSH transport uses the following data integrity MAC algorithms: hmac-sha2-256 and hmac-sha2-512 • Key exchange algorithms supported are: ecdh-sha2-nistp256 and ecdh-sha2-nistp384. • The TOE ensures that during SSH connections, the same session keys are used for a threshold of no longer than one hour and no more than one gigabyte of transmitted data

4.3 Identification and Authentication

All users must be authenticated by the TOE prior to carrying out any administrative actions. The TOE supports password-based and public-key based authentication. An administrator can set a minimum password length on the TOE which must be at least 15 characters. This is true of users accessing the TOE via the local console, or through protected paths using the remote CLI via SSH. Users can authenticate to the TOE using a username and password. In addition, when authenticating by the remote CLI, users can instead use SSH public-key authentication. Passwords can consist of upper-case letters, lower-case letters, numbers, and a set of selected special characters. Password information is never revealed during the authentication process including during login failures. Before a user authenticates the device, a customizable warning banner is configured to be displayed.

4.4 Security Management

The TOE supports local and remote management of its security functions including:

- Local console CLI administration
- Remote CLI administration via SSHv2
- Configurable banner displayable at login
- Timeouts to terminate administrative sessions after a set period of inactivity
- Timed user lockout after multiple failed authentication attempts
- Configurable authentication failure parameters
- Re-enabling locked accounts
- Configurable cryptographic parameters

The administrative user can perform all the above security-related management functions.

4.5 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys, and private keys from unauthorized disclosure. Passwords are stored as SHA 512 hashes. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. The TOE internally maintains the date and time. An administrator can install software updates to the TOE after they are verified using a digital signature mechanism.

4.6 TOE Access

The TOE displays a customizable banner before any administrative session can be established with it. The TOE will terminate local or remote interactive sessions after a specified period of session inactivity configured by an administrator. An administrator can terminate their own interactive local or remote sessions.

The local and remote CLI interfaces display the default security banner prior to authentication that is also configurable. The TOE can terminate local CLI and remote CLI sessions after a specified time-period of inactivity. Administrative users have the capability to terminate their own sessions.

4.7 Trusted Path/Channels

The TOE supports SSH for secure communications with authorized IT entities such as syslog servers. The TOE supports SSHv2 (remote CLI) for secure remote administration.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 4 – Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or cPP_ND_v3.0e, 06-Dec-2023 41 interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

ID	Assumption
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 5 – Threats

ID	Threat
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

ID	Threat
	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. Nonvalidated 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

ID	Threat
	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. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
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.

5.3 Clarification of Scope

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

- As with any evaluation, this evaluation 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 3.0e, 06 December 2023 [CPP_ND_V3.0E] and Functional Package for SSH, Version 1.0, 13 May 2021 [PKG_SSH_v1.0].

- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following document was provided by the vendor with the TOE for evaluation:

- Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3 Operational User Guidance, Version 0.7, May 2025

Only the Administrator's Guide listed above, and the specific sections of the other documents referenced by that guide should be trusted for the installation, administration, and use of this product in its evaluated configuration.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

This section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references. The specific testbed configuration including architecture and relevant IP addresses and port numbers of the systems are described in the AAR section 2.1.

All TOE models below run the same Klas Keel 5.4.3 binary file. The TOE supports SSH functionality for both management and export of logging information.

Table 6 – TOE Model

TOE Model	Specifications
VoyagerVM 4.0 	Xeon D-1746TER Intel(R) Xeon(R) Ice Lake D-1746TER 10-Core CPU @ 2.00GHz with 128GB RAM Intel® Xeon® D-1712TR Processor 4-Core CPU @ 2.00GHz with 128GB RAM Network Ports: ° 4 x 25 Gbps SFP28 interfaces ° 2 x 2.5 Gbps RJ45 Ethernet ports ° 1 x RJ45 Ethernet for management ° 1 x RJ45 Serial console port Network Ports: 1 x console, 2 x 10 GB SFP, 2 x 1GB ethernet Storage: · 2 x E1.S 9.5mm NVMe SED SSDs · 1 x VIK+ NVMe boot or write-cache device · 1 x 256 GB NVMe internal boot device (optional)

7.1.1 Physical Boundaries

The TOE boundary is the hardware appliance which is comprised of hardware and the KlasOS Keel software component. The TOE hardware model is provided in **Table 6 – TOE Model**.

The TOE also supports secure connectivity with several other IT environment devices, including the ones identified in the following table.

The TOE implements SSHv2 to protect the remote management interface for administrators.

7.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

Table 7 – Excluded Functionality

Components	Exclusion Rationale
SNMP	Remote management is performed using SSH
Spanning-Tree	Spanning-Tree is not used in the evaluated configuration
TACACS+	TACACS+ is not used for authentication on the TOE
Port Security	Port Security is not used in the evaluated configuration
RADIUS	RADIUS is not used in the evaluated configuration
SD-WAN	SD-WAN using the DTLS protocol is not enabled in the evaluated configuration
Firewall Functionality	The Firewall functionality is disabled in the evaluated configuration

8 IT Product Testing

This section summarizes the testing efforts of the evaluation team. Section 2.1 of the AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] and Functional Package for SSH, Version 1.0, 13 May 2021 [PKG_SSH_v1.0]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8.3 Test Information and Location

All testing was performed by George Kumi and Alexander Fannin at the Acumen Security office located at 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from August 2024 to May 2025.

9 Results of the Evaluation

The evaluation was conducted based upon CC version 3.1 Rev. 5 and CEM version 3.1 Rev. 5. The evaluation determined the Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

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 Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] and Functional Package for SSH, Version 1.0, 13 May 2021 [PKG_SSH_v1.0].

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 Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] and Functional Package for SSH, Version 1.0, 13 May 2021 [PKG_SSH_v1.0] related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 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 Assurance

Activities specified in the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] and Functional Package for SSH, Version 1.0, 13 May 2021 [PKG_SSH_v1.0] related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 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 Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] and Functional Package for SSH, Version 1.0, 13 May 2021 [PKG_SSH_v1.0] and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator 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 collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] and Functional Package for SSH, Version 1.0, 13 May 2021 [PKG_SSH_v1.0], and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 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 following sources were searched during the evaluation:

- https://nvd.nist.gov/view/vuln.search

The searches were performed on 5/1/2025 with the following keywords:

- (OpenSSH 9.9p1) cpe:/:openbsd:openssh:9.9
- (GNU C Library 2.31) cpe:2.3:a:gnu:glibc:2.31:*:*:*:*:*:*:*
- (OpenSSL 3.0.8) cpe:/:openssl:openssl:3.0.8

- (Linux-PAM 1.3.1) cpe:/:linux-pam:linux-pam:1.3.1
- (rsyslogd 8.34.0) cpe:/:rsyslog:rsyslog:8.34.0
- (chronyd 3.4) cpe:/:chrony_project:chrony:3.4
- (KlasOS Keel v5.4.3)
- (Klas Voyager VM4.0)
- (Ice Lake D-1746TER) cpe:/:intel:xeon_d-1746ter
- (Ice Lake D-1712TR) cpe:/:intel:xeon_d-1712tr

The search was performed on 1/14/25, 3/31/25, and a follow up search performed on 5/30/25. All vulnerabilities were retrieved from https://nvd.nist.gov/vuln/search. No open vulnerabilities applicable to the TOE were 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 addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] and Functional Package for SSH, Version 1.0, 13 May 2021 [PKG_SSH_v1.0], 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 Assurance Activities in the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] and Functional Package for SSH, Version 1.0, 13 May 2021 [PKG_SSH_v1.0], 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 guidance documents listed in Section 6 of this report. 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 and no further conclusions can be drawn about their effectiveness. See Section 7.2 of this report for product functionality that is not included in the scope of evaluation. No other versions of the TOE, either earlier or later, were evaluated.

Additional functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other items and scope issues have been sufficiently addressed in other sections of this document.

11 Annexes

Not applicable.

12 Security Target

Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3 Security Target, Version 1.1, 16 May 2025.

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. *Assurance Activity Report for Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3*, Version 1.1, 16 May 2025
2. *collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023 [CPP_ND_V3.0E].
3. *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model*, Version 3.1 Revision 5.
4. *Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements*, Version 3.1 Revision 5.
5. *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements*, Version 3.1 Revision 5.
6. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5.
7. *Evaluation Technical Report for Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3*, Version 1.5, 16 May 2025. (Proprietary)
8. *Functional Package for SSH*, Version 1.0, 13 May 2021 [PKG_SSH_v1.0].
9. *Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3 Operational User Guidance*, Version 0.7, May 2025.
10. *Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3 Security Target*, Version 1.1, 16 May 2025.
11. *Master Test Report for Klas VoyagerVM 4.0 Running KlasOS Keel 5.4.3*, Version 1.2, 23 May 2025. (Proprietary)
12. *Assurance Activity Report for Klas VoyagerVM 4.0 Running KlasOS Keel 5.4.3*, Version 1.2, 16 May 2025.
13. *Vulnerability Assessment for Klas VoyagerVM 4.0 running KlasOS Keel 5.4.3*, Version 0.4, May 30, 2025.