

National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme



Validation Report Infinera Corporation Transcend Network Management System Client 18.10.3

Report Number: CCEVS-VR-11318-2022
Dated: December 8, 2022
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

Sheldon Durrant
Lauren Hardy
Randy Heimann
Linda Morrison
Clare Parran
The MITRE Corporation

Common Criteria Testing Laboratory

Raymond Smoley
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1	Executive Summary	1
2	Identification	2
3	Assumptions & Clarification of Scope	3
4	Architectural Information	4
4.1	TOE Evaluated Platforms	4
4.2	TOE Architecture	4
4.3	Physical Boundaries	4
5	Security Policy	5
5.1	Cryptographic support	5
5.2	User data protection	5
5.3	Identification and authentication	5
5.4	Security management	5
5.5	Privacy	6
5.6	Protection of the TSF	6
5.7	Trusted path/channels	6
6	Documentation	7
7	Evaluated Configuration	8
8	IT Product Testing	9
8.1	Developer Testing	9
8.2	Evaluation Team Independent Testing	9
9	Results of the Evaluation	10
9.1	Evaluation of the Security Target (ASE)	10
9.2	Evaluation of the Development (ADV)	10
9.3	Evaluation of the Guidance Documents (AGD)	10
9.4	Evaluation of the Life Cycle Support Activities (ALC)	11
9.5	Evaluation of the Test Documentation and the Test Activity (ATE)	11
9.6	Vulnerability Assessment Activity (VAN)	11
9.7	Summary of Evaluation Results	12
10	Validator Comments/Recommendations	13
11	Annexes	14
12	Security Target	15
13	Glossary	16
14	Bibliography	17

List of Tables

Table 1: Evaluation Identifiers	2
Table 2: Glossary	16

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Infinera Transcend Network Management System Client solution provided by Infinera Corporation. 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 December 2022. 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 Extended and meets the assurance requirements of the Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) with the Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11).

The Target of Evaluation (TOE) is the Infinera Corporation Transcend Network Management System Client 18.10.3. 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 Infinera Corporation Transcend Network Management System Client 18.10.3 Security Target, Version 1.5, December 6, 2022 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Infinera Transcend Network Management System Client 18.10.3
Protection Profile	Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) with the Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11)
ST	Infinera Corporation Transcend Network Management System Client 18.10.3 Security Target, Version 1.5, December 6, 2022
Evaluation Technical Report	Evaluation Technical Report for Infinera Corporation Transcend Network Management System Client 18.10.3, version 0.3, December 6, 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
Sponsor	Infinera Corporation
Developer	Infinera Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Sheldon Durrant, Lauren Hardy, Randy Heimann, Linda Morrison, Clare Parran

Table 1: Evaluation Identifiers

3 Assumptions & Clarification of Scope

Assumptions

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

- Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14)
- Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11)

That information has not been reproduced here and the ASPP14/PKGTLS11 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 ASPP14/PKGTLS11 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.

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 Application Software Protection Profile with the TLS 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 Software Application 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 ASPP14/PKGTLS11 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

4 Architectural Information

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

The Transcend Network Management System (TNMS) is designed to provide end-to-end network and service management across multiple technologies and equipment vendors. For purposes of this evaluation, the TNMS Client is a software application that offers a secure web-based user interface to its users and in turn securely communicates management instructions to a configured TNMS Server.

Note that the full TNMS system consists of client and server components, this evaluation is limited only to the client components since the Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) does not support the evaluation of distributed application solutions.

4.1 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 7 below.

4.2 TOE Architecture

The TNMS Client is a single Java application designed to run in the following operational environment:

- Microsoft Windows 10 (64 bit) on a 64 bit Intel Xeon processor
- Amazon Corretto (OpenJDK) JDK/JRE 11.0.6
- Oracle Java JRE 8u201

The TNMS Client provides a graphical user-interface to its users so that they can perform management functions. The TNMS Client implements a TLS client to connect to the TNMS Server so that management instructions can be processed and forwarded as necessary to network entities.

The secure communication features all utilize Bouncy Castle (installed as part of the TNMS Client) for cryptographic operations.

4.3 Physical Boundaries

The TNMS Client TOE is a single Java application running on Amazon Corretto (OpenJDK) JDK/JRE version 11.0.6 and Oracle Java JRE 8u201 JRE operating in a Microsoft Windows 10 (64 bit) environment. The only external services the TOE depends on are a Certificate Authority for X509 certificate validation services and the TNMS Server with which the TNMS Client is configured to work.

5 Security Policy

This section summarizes the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Privacy
6. Protection of the TSF
7. Trusted path/channels

5.1 Cryptographic support

The TOE uses Automated Cryptographic Validation Test System (ACVTS)-validated cryptographic algorithm implementations, provided by its Bouncy Castle cryptographic module installed with the TOE, to support asymmetric key generation, encryption/decryption, signature generation and verification and establishment of trusted channels to protect data in transit. The TOE implements a TLS client to securely communicate with a TNMS Server. The TOE also relies on the underlying Java Runtime Environment to generate entropy that is used as input data for the TOE's deterministic random bit generator (DRBG).

5.2 User data protection

The TOE does not access any hardware resources or sensitive information repositories and no sensitive data is stored in non-volatile memory. Inbound and outbound network communications are restricted to those that are user-initiated.

5.3 Identification and authentication

The TOE implements X509 certificate validation to validate the revocation status of certificates using CRL. The TOE uses X509 certificates to support TLS authentication.

5.4 Security management

The TOE provides a graphical user interface to operate the TOE.

The TOE requires no management beyond configuration of the URI of the TNMS server to which it connects and the root CA certificate to which the TNMS server's peer certificate should chain.

When configured with default credentials or no credentials, the TOE restricts its functionality and only allows the ability to set new credentials. By default, the TOE is configured with file permissions to protect itself and its data from unauthorized access.

5.5 Privacy

The TOE does not transmit personally identifiable information (PII) over any network interfaces.

5.6 Protection of the TSF

The TOE protects itself against exploitation by implementing address space layout randomization (ASLR) and by not allocating any memory region for both write and execute permission. The TOE uses standard platform APIs and includes a number of third party libraries used to perform its functions.

The TOE includes mechanisms to check for updates and to query the current version of the application software. TOE software is digitally signed and distributed using the platform-supported package manager. The TOE does not update its own binary code in any way and when removed, all traces of the TOE application software are deleted.

5.7 Trusted path/channels

The TOE protects communications between itself and remote administrators using TLS and between itself and the TNMS Server using TLS.

6 Documentation

The following documents were available with the TOE for evaluation:

- Infinera Transcend Network Management System Client 18.10.3 Administrative Guidance for Common Criteria, Version 1.2, December 6, 2022

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 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 Evaluated Configuration

The TNMS Client is a single Java application designed to run in the following operational environment:

- Microsoft Windows 10 (64 bit) on a 64 bit Intel Xeon processor
- Amazon Corretto (OpenJDK) JDK/JRE 11.0.6
- Oracle Java JRE 8u201

The TNMS Client provides a graphical user-interface to its users so that they can perform management functions. The TNMS Client implements a TLS client to connect to the TNMS Server so that management instructions can be processed and forwarded as necessary to network entities.

The secure communication features all utilize Bouncy Castle (installed as part of the TNSM Client) for cryptographic operations.

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 proprietary Detailed Test Report for Infinera Corporation Transcend Network Management System Client, Version 0.3, December 6, 2022 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

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 a Common Criteria Certification document and ran the tests specified in the ASPP14/PKGTLS11 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.

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 Transcend Network Management System Client TOE to be Part 2 extended, and to meet the SARs contained in the ASPP14/PKGTLS11.

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 Infinera Transcend Network Management System Client 18.10.3 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 and Guidance documents. Additionally the Evaluators performed the assurance activities specified in the ASPP14/PKGTLS11 related to the examination of the information contained in the TSS.

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.

9.3 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 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.

9.4 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 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 ASPP14/PKGTLS11 and recorded the results in a Test Report, summarized in the AAR.

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.

9.6 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 vulnerabilities.

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/>) on 12/01/2022 with the following search terms:

- Infinera
- Infinera Corporation
- Transcend Network Management System
- TNMS
- Apache Xerces
- AdventNet
- AOP Alliance
- Apache Active MQ
- Apache Avalon
- Apache Commons
- Apache FOP
- Apache FTP server
- Apache HttpClient
- Apache ORO
- Apache Tomcat
- Apache Velocity
- Apache XML
- Apached Commons Codec
- ASM
- AspectJ
- Batik
- Bouncy Castle
- Castor
- cglib
- Disruptor
- Docking Frames
- Dom4j
- EdDSA
- edftpj
- EHCache
- Ganymed
- Guice
- google-collection
- gson
- Guava
- image4j
- InstallAnywhere
- io.grpc
- istack common
- Jakarta Activation
- Jakarta Mail
- Java Architecture for XML Binding
- Java Communications
- Java FX
- Java Swing
- javaee/glassfish V2 Milestone
- JavaHelp
- Javax Inject
- JavaZoom Basic Player
- JaxB Runtime
- JCalendar
- JDOM
- Jersey
- JFreeChart
- JFreeReport
- jgraphx
- JIDE
- Jlayer
- Jscape
- JSch
- JSR305
- JUnit
- json
- Log4J
- MiGLayout
- MP3SPI
- OpenCensus
- OpenMap
- OpenProps
- Oracle Database JDBC Drivers
- Plexus
- reactive-streams
- reflections
- rxjava
- SLF4J
- snappy
- SNMP4j
- SSHJ
- Tritonus
- VorbisSPI
- VT Dictionary
- VT Password
- webdavilb
- webdavlib
- Wildfly
- Xalan
- XBean
- XML Commons.

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.

9.7 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 Infinera Transcend Network Management System Client 18.10.3 Administrative Guidance for Common Criteria, Version 1.2, December 6, 2022. 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. All other functionality provided by devices in the operational environment, 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 is identified as: Infinera Corporation Transcend Network Management System Client 18.10.3 Security Target, Version 1.5, December 6, 2022.

13 Glossary

The following definitions are used throughout this document:

Term	Definition
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.

Table 2: Glossary

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] Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14).
- [5] Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 (PKGTLS11).
- [6] Infinera Corporation Transcend Network Management System Client 18.10.3 Security Target, Version 1.5, December 6, 2022 (ST).
- [7] Assurance Activity Report for Infinera Corporation Transcend Network Management System Client 18.10.3, Version 0.3, December 6, 2022 (AAR).
- [8] Detailed Test Report for Infinera Corporation Transcend Network Management System Client, Version 0.3, December 6, 2022 (DTR).
- [9] Evaluation Technical Report for Infinera Corporation Transcend Network Management System Client 18.10.3, Version 0.3, December 6, 2022 (ETR).
- [10] Infinera Transcend Network Management System Client 18.10.3 Administrative Guidance for Common Criteria, Version 1.2, December 6, 2022 (AGD).