

National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme



Validation Report for the Dell Networking SmartFabric OS10.6

Report Number: CCEVS-VR-VID11679-2026
Dated: September 30, 2026
Version: 1.0

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

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

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers

Marybeth Panock

Dale Schroeder

Aerospace Corporation (FFRDC)

Common Criteria Testing Laboratory

Joon Sim

Lightship Security USA, Inc.

Table of Contents

1. Executive Summary	3
2. Identification.....	4
3. Architectural Information	6
3.1. TOE Evaluated Configuration	7
3.2. Physical Boundary	7
3.3. Required Non-TOE Hardware, Software, and Firmware	8
4. Security Policy	8
4.1. Security Audit.....	9
4.2. Cryptographic Support.....	9
4.3. Identification and Authentication.....	10
4.4. Security Management	10
4.5. Protection of the TSF.....	10
4.6. Trusted Path/Channels	11
5. Assumptions, Threats, Clarification of Scope	11
5.1. Assumptions.....	12
5.2. Threats.....	12
5.3. Clarification of Scope	14
6. Documentation.....	14
7. Evaluated Configuration	15
7.1. Evaluated Configuration	16
7.2. Excluded Functionality	16
8. IT Product Testing	16
8.1. Developer Testing	17
8.2. Evaluation Team Independent Testing	17
8.3. Evaluation Team Testing Environment	17
9. Results of the Evaluation	19
9.1. Evaluation of Security Target (ASE).....	20
9.2. Evaluation of Development Documentation (ADV).....	20
9.3. Evaluation of Guidance Documents (AGD).....	20
9.4. Evaluation of Life Cycle Support Activities (ALC).....	21
9.5. Evaluation of Test Documentation and the Test Activity (ATE)	21

9.6. Vulnerability Assessment Activity (VAN).....	21
9.7. Summary of Evaluation Results.....	23
10. Validator Comments	23
11. Annexes.....	24
12. Security Target.....	25
13. Glossary	26
14. Acronym List	27
15. Bibliography.....	28
Figure 1: TOE in the Operational Environment	4
Figure 2: Example of TOE Deployment	13
Table 1: Evaluation Identifiers.....	2
Table 2: Test Systems	13
Table 3: Tools Used for Testing	14

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Dell Networking SmartFabric OS10.6 provided by Dell Technologies Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in September, 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices, v3.0e and Functional Package for SSH, v1.0.

The TOE is Dell Networking SmartFabric OS10.6. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 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 (CCEVS) and the conclusions of the testing laboratory in the ETR 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Security Target 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.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	Dell Networking SmartFabric OS10.6
Sponsor and Developer	Dell Technologies Inc. One Dell Way Round Rock TX, 78682
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	Collaborative Protection Profile for Network Devices, v3.0e Functional Package for SSH, v1.0
ST	Dell Networking SmartFabric OS10.6 Security Target, v1.1
Evaluation Technical Report	Dell Networking SmartFabric OS10.6 Evaluation Technical Report, v1.1
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Lightship USA: Joon Sim
CCEVS Validators	Aerospace Corporation: Jerome Myers, Marybeth Panock, Dale Schroeder

3. Architectural Information

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

Dell Networking SmartFabric OS10.6 is a network switch. The TOE is deployed within a network to provide layer 2 and layer 3 network management and interconnectivity functionality. The TOE interfaces within the scope of evaluation.

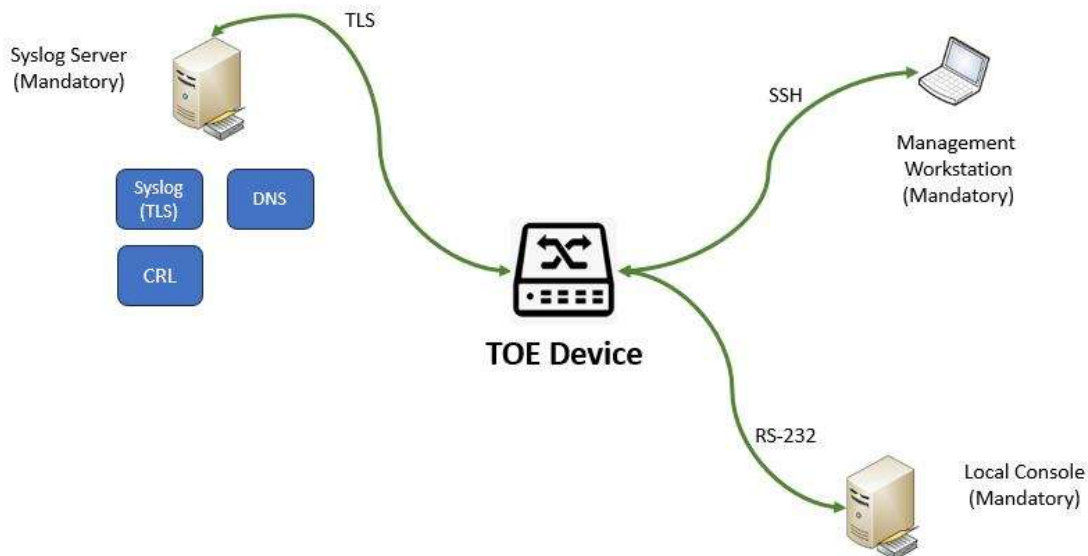
3.1.1. TOE Evaluated Configuration

The TOE is deployed within a network to provide layer 2 and layer 3 network management and interconnectivity functionality. The device configuration determines how packet flows and management traffic are handled across the TOE's network interfaces.

An external syslog server must be used to store audit records, with log data protected and transmitted securely via Syslog over TLS. Secure remote administration is supported via SSH (SSHv2), which is implemented with authentication failure handling. Additionally, local administrative management is supported via a direct physical serial connection.

The following figure provides a visual depiction of an example TOE deployment:

Figure 1: TOE in the Operational Environment



3.1.2. Physical Boundary

The physical boundary of the TOE includes all software and hardware shown in table below. TOE is delivered via commercial courier.

Type	Model	CPU	Software	CAVP
Physical	S4112F-ON S4112T-ON S4128F-ON S4128T-ON S4148F-ON S4148T-ON MX5108n	Intel Atom C2338 (Silvermont)	Dell Networking SmartFabric OS 10.6.1	A8619
	S5212F-ON N3248TE-ON	Intel Atom C3338 (Denverton)		
	S5224F-ON S5232F-ON S5248F-ON S5296F-ON	Intel Atom C3538 (Goldmont)		
	Z9432F-ON S5448F-ON	Intel Atom C3758 (Goldmont)		
	E3224F-ON S3248T-ON	Intel Atom C3558/C3558R (Goldmont)		
	Z9664F-ON	Intel Xeon D-1714 (Ice Lake)		

3.1.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

- Audit Server. The TOE can send audit events to a Syslog server.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1.1. Security Audit

The TOE generates audit records of security-relevant events, including user and administrator actions, and logs these events locally. Each audit event includes identity of the user responsible for the action, when applicable. Additionally, the Security Administrator can configure the TOE to send logs in real-time to a syslog server via TLS.

4.1.2. Cryptographic Support

The TOE implements a cryptographic module. The cryptographic module has the ability to generate and destroy cryptographic keys. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in table below.

CAVP Certificates

SFR	Algorithm(s) (Keys/curves/digest-size)	Standard	Usage	Module	Certificate
FCS_COP.1/Data Encryption	AES-CTR (128, 256-bit)	ISO 18033-3, ISO 10116	SSH	Dell FIPS Module based on the OpenSSL FIPS Provider v3.1.2	A8619
FCS_COP.1/Data Encryption	AES-GCM (128, 256-bit)	ISO 18033-3, ISO 19772	SSH, TLS		
FCS_CKM.1	RSA KeyGen 2048, 3072, 4096-bit	FIPS PUB 186-4 / FIPS PUB 186-5	SSH, TLS		
FCS_COP.1/ SigGen	RSA SigGen 2048, 3072, 4096-bit RSA SigVer 2048, 3072, 4096-bit	FIPS PUB 186-4 / FIPS PUB 186-5, ISO/IEC 9796-2	SSH, TLS, Update Verification		
FCS_CKM.1	ECDSA KeyGen P-256, P-384, P-521	FIPS PUB 186-4 / FIPS PUB 186-5, ISO/IEC 14888-3	SSH, TLS		
FCS_COP.1/ SigGen	ECDSA SigGen P-256, P-384, P-521 ECDSA SigVer P-256, P-384, P-521	FIPS PUB 186-4 / FIPS PUB 186-5, ISO/IEC 14888-3, NIST SP 800-186	SSH, TLS		
FCS_COP.1/Hash	SHA-256 (256-bit digest),	ISO/IEC 10118-3:2004	TLS, SSH, Password Storage,		

SFR	Algorithm(s) (Keys/curves/digest-size)	Standard	Usage	Module	Certificate
	SHA-384 (384-bit digest), SHA-512 (512-bit digest)		Update Verification		
FCS_COP.1/ KeyedHash	HMAC-SHA-256 (256-bit key/digest), HMAC-SHA-512 (512-bit key/digest)	ISO/IEC 9797- 2:2011 Section 7	TLS, SSH		
FCS_CKM.1 FCS_CKM.2	KAS-ECC P-256, P-384, P-521	NIST SP 800-56A Revision 3	SSH, TLS		
FCS_RBG_EXT.1	Counter DRBG (AES-256)	ISO/IEC 18031:2011	Entropy source		

4.1.3. Identification and Authentication

The TOE ensures that all users must be authenticated before accessing its functions and data. TOE can be accessed directly via serial RJ45 connection or remotely via SSHv2 connection. When a user account has sequentially failed authentication the configured number of times, the account will be locked for a Security Administrator defined time period. The TOE uses X.509v3 certificates to support authentication for TLS. Certificate revocation checking is performed using a CRL.

4.1.4. Security Management

The TOE enables secure management of its security functions, including:

- a) Administrator authentication with passwords
- b) Configurable password policies
- c) Role Based Access Control
- d) Access banners
- e) Management of critical security functions and data
- f) Protection of cryptographic keys and passwords

4.1.5. Protection of the TSF

The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions. The TOE performs diagnostic self-tests and cryptographic module self-tests during start-up and generates audit records to record a failure. Self-tests comply with the FIPS 140-2 requirements for self-testing.

Note. For the evaluated configuration, Secure Boot must be enabled in the system BIOS.

4.1.6. Trusted Path/Channels

The TOE protects the integrity and confidentiality of communications using secure protocols as noted in section 3.1 above, and using cryptographic algorithms as described in the table in section 4.2.

5. Assumptions, Threats, Clarification of Scope

5.1.1. Assumptions

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

- collaborative Protection Profile for Network Devices, Version 3.0e
- Functional Package for Secure Shell (SSH), v1.0

That information has not been reproduced here and CPP_ND_V3.0E and PKG_SSH_V1.0 should be consulted if there is interest in that material.

5.1.2. 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.

Identifier	Description
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

5.1.3. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V3.0E and PKG_SSH_V1.0 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.

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 in accordance with the evaluation activities specified in CPP_ND_V3.0E and PKG_SSH_V1.0 and performed by the Evaluation team
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- 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 CPP_ND_V3.0E and PKG_SSH_V1.0 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Dell Networking SmartFabric OS10.6 Common Criteria Guide, Version 1.0, August 2026*
- *Dell SmartFabric OS10 User Guide, Release 10.6.1 April 2026 Rev. A00*

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.

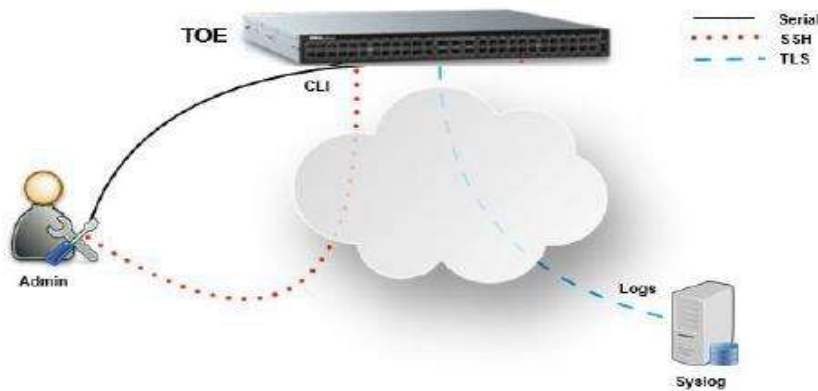
To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7. EVALUATED CONFIGURATION

7.1.1. Evaluated Configuration

The TOE is a network switch which is deployed within a network to provide layer 2 and layer 3 network management and interconnectivity functionality. The TOE interfaces within the scope of evaluation are shown in the Figure 2 below. The evaluated configuration is also described in the Dell Networking SmartFabric OS10.6 Common Criteria Guide Sections 1.3.2 Evaluated Software and Hardware and 1.3.3 Evaluated Functions..

Figure 2: Example of TOE Deployment



The TOE interfaces are as follows:

- a) CLI. Administrative CLI via direct serial connection or SSH.
- b) Logs. Syslog via TLS.

7.1.2. Excluded Functionality

The evaluation is limited to those security functions identified in Security Target Section Security Functions / Logical Scope 2.3. Switching and software defined networking functions are outside the scope of TOE security functions.

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Dell Networking SmartFabric OS10.6 Assurance Activity Report, v1.1, September 2026* provides an overview of testing and the prescribed evaluation activities.

8.1.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

8.1.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from December 2025 until September 2026. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

8.1.3. Evaluation Team Testing Environment

The TOE testing environment components are identified Table 2 ‘Test Systems’, and Table 3 ‘Tools Used for Testing’ shown below.

Table 2: Test Systems

Name / HW / SW	Description / Functions	Test Tools
S5212F-ON HW: S5212F-ON SW: OS10.6.1.1	Fully tested TOE model TLS SSH	N/A
Services VM HW: Test Hypervisor SW: Debian 10	Logging Server (TLS) DNS Server CRL Distribution Point Perform Packet Captures	syslog-ng 3.19.1-5+deb10u1 dnsmasq 2.80-1+deb10u1 OpenSSH 7.9p1-10+deb10u2 Python 2.7.16-1
GL VM HW: Test Hypervisor SW: Kali 2023.2	SSH Client (SSH) Protocol Test Host (TLS/SSH) Certification Authority	Greenlight 3.0.35 Python 3.11.2 OpenSSL 3.5.4

Name / HW / SW	Description / Functions	Test Tools
	Perform Packet Captures	OpenSSH 10.2p1-3 Wireshark 4.0.3-1 tcpdump 4.99.3-1
Test Hypervisor HW: Dell PowerEdge R440 SW: ESXi, 7.0.3	Hypervisor for the Services VM and Management Workstation	None
Netgear Switch HW: ProSafe Plus GS105E	Physical disconnect packet captures	N/A
Packet Capture Laptop HW: Lenovo ThinkPad T15 SW: Windows 11 Pro	Physical disconnect packet captures	Wireshark 4.6.3

Table 3: Tools Used for Testing

Tool name	Version	Description
Lightship Greenlight	3.0.35 (GL VM)	Tool used for TLS/X509 certificate modification as well as handshake modification
OpenSSL	3.5.4 (GL VM)	OpenSSL was used for simple TLS server or TLS client connections and as an OCSP responder
Wireshark	4.0.3-1 (GL VM) 4.6.3 (Windows)	Used for packet capture and analysis
OpenSSH	10.2p1-3 (GL VM)	SSH client for accessing the Remote CLI
dnsmasq	2.80-1+deb10ui (Services VM)	DNS server
Syslog-ng	3.19.1-5+deb10u1	Syslog server

Tool name	Version	Description
Python	2.7.16-1 (Services VM) 3.11.2 (GL VM)	HTTP server
Tcpdump	4.99.3-1 (GL VM)	Used for packet capture and analysis

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 documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined Dell Networking SmartFabric OS10.6 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in CPP_ND_V3.0E and PKG_SSH_V1.0.

9.1.1. Evaluation of 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 Dell Networking SmartFabric OS10.6 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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.

9.1.2. Evaluation of Development Documentation (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 ST and Guidance documents. Additionally, the evaluator performed the Evaluation Activities related to the examination of the information contained in the TSS.

The Validation 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.

9.1.3. Evaluation of 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 Validation team 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.

9.1.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team 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.

9.1.5. Evaluation of 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 Test Evaluation Activities and recorded the results in a Test Report, summarized in the AAR.

The Validation team 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.

9.1.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Dell Networking SmartFabric OS10.6 Vulnerability Assessment, v0.6, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on August 10, 2026, did not uncover any residual vulnerability. The searches were updated on September 10, 2026.

The Evaluation team searched:

- Dell security advisories (<https://www.dell.com/support/security/en-us>)
- CISA - Known Exploited Vulnerabilities Catalog: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): <https://web.nvd.nist.gov/view/vuln/search>
- Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
- CVE Details: <https://www.cvedetails.com/vulnerability-search.php>

The Evaluation team performed a search using the following keywords:

- Dell Networking SmartFabric OS 10.6

- S4112F-ON
- S4112T-ON
- S4128F-ON
- S4128T-ON
- S4148F-ON
- S4148T-ON
- MX5108n
- S5212F-ON
- N3248TE-ON
- S5224F-ON
- S5232F-ON
- S5248F-ON
- S5296F-ON
- Z9432F-ON
- S5448F-ON
- E3224F-ON
- S3248T-ON
- Z9664F-ON
- Intel Atom C2338 (Silvermont)
- Intel Atom C3338 (Denverton)
- Intel Atom C3538 (Denverton)
- Intel Atom C3758 (Denverton)
- Intel Atom C3558 (Denverton)
- Intel Atom C3558R (Denverton)
- Intel Xeon D-1714 (Ice Lake)
- auditd
- bash
- bind9
- curl
- glib2.
- glibc
- gnupg2
- iptables
- ivykis
- krb5

- libbsd
- libcap-ng
- libcap2
- libgcrypt20
- libgpg
- libnl3
- libzstd
- lz4
- net-snmp
- openssl
- OpenSSL FIPS Object Module
- pam
- pciutils
- pcre2
- pcre3
- perl
- pkixssh
- radsecproxy
- syslog-ng
- systemd
- tcpd
- xz-utils
- openssh
- libssh
- libssh2

The Validation team 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.

9.1.7. 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 followed the procedures defined in the CEM and

performed the Evaluation Activities in CPP_ND_V3.0E and PKG_SSH_V1.0, 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 documentation referenced in Section 6 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. 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.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Section 7.2 of this document, and Section 2.4.3 “Functions not included in the TOE Evaluation” of the ST, identify the features that are part of the purchased product but were not included in the evaluation. Notably, these non-evaluated functions include switching and software defined networking functions. These are outside the scope of TOE security functions.

Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

11. Annexes

Not applicable.

12. Security Target

Dell Networking SmartFabric OS10.6 Security Target, v1.1, September 2026

13. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional requirements, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance requirements, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
5. collaborative Protection Profile for Network Devices, Version: 3.0e, December 06, 2023
6. Functional Package for Secure Shell (SSH), Version 1.0, May 13, 2021
7. Dell Networking SmartFabric OS10.6 Security Target, v1.1, September 2026 **(ST)**
8. Dell Networking SmartFabric OS10.6 Common Criteria Guide, v1.0, August 2026 **(AGD)**
9. Dell SmartFabric OS10 User Guide Release 10.6.1, April 2026 Rev. A00
10. Dell Networking SmartFabric OS10.6 Assurance Activity Report, v1.2, September 2026 **(AAR)**
11. Dell Networking SmartFabric OS10.6 Vulnerability Assessment, v1.1, September 2026 **(AVA)**
12. Dell Networking SmartFabric OS10.6 Evaluation Technical Report, v1.2, September 2026 **(ETR)**
13. Dell Networking SmartFabric OS10.6 NDcPPv3.0e/PKG_SSH Detailed Test Report, v1.1, September 2026 **(DTR)**
14. Dell Networking SmartFabric OS10.6 NDcPPv3.0e/PKG_SSH Detailed Test Evidence, v1.1, September 2026