National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Fortinet, Inc.

FortiSandbox 4.4

Report Number: CCEVS-VR-VID11636-2025
Dated: October 31, 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

Acknowledgements

Validation Team

Linda Morrison
Lisa Mitchell (Senior)
Lori Sarem
Jaemond Reyes
Randy Heimann (Lead)

The MITRE Corporation

Common Criteria Testing Laboratory

Michael Baron
Meghana Achanta
Dylan Lyman
Oleg Andrianov

UL Verification Services Inc.
San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the FortiSandbox 4.4 by Fortinet, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by UL Verification Services Inc., a Common Criteria Testing Laboratory (CCTL) in San Luis Obispo, CA, United States of America, and was completed September 26, 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by UL Verification Services Inc. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the *collaborative Protection Profile for Network Devices*, Version 3.0e, dated December 6, 2023 with *Functional Package for Secure Shell (SSH),* Version: 1.0, May 13, 2021.

The Target of Evaluation (TOE) is the FortiSandbox 4.4.

When installed as a physical network appliance, the TOE's evaluated configuration is a standalone network device. When installed as a virtual network appliance, the TOE's evaluated configuration is a virtual network device.

The TOE 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 (CCEVS). 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). 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 *FortiSandbox 4.4 Security Target*, Version v1.6, October 30, 2025 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 who desire 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.

Evaluation Scheme	United States NIAP Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	FortiSandbox 4.4
Protection Profile	*collaborative Protection Profile for Network Devices,* Version 3.0e, dated December 6, 2023 with *Functional Package for Secure Shell (SSH)*, Version: 1.0, 2021-05-13
Security Target	*FortiSandbox 4.4 Security Target*, version 1.6, October 30 2025
Dates of Evaluation	December 2024 - October 2025
Conformance Result	Pass
Common Criteria Version	CC Version 3.1r5, April 2017
Common Evaluation Methodology (CEM) Version	CEM Version 3.1r5, April 2017
Evaluation Technical Report (ETR)	*Common Criteria Evaluation Technical Report*, UL15437480-ETR v1.2, October 28, 2025
Sponsor/Developer	Fortinet, Inc.
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc. San Luis Obispo, CA
CCEVS Validators	Randy Heimann, Lisa Mitchell, Linda Morrison, Jaemond Reyes, Lori Sarem

Table 1: Product Identification

3 Assumptions and Clarification of Scope

3.1 Assumptions

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

- *collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021

That information has not been reproduced here and the Protection Profiles should be consulted if there is interest in that material.

3.2 Clarification of Scope

The evaluation of security functionality and scope are inherently tied to the specific assurance activities performed and the defined scope of the evaluation methodology. This evaluation provides no assurance that the TOE counters any threats which are not identified in the above Protection Profiles. 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 clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- This evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and performed by the evaluation team).

- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Network device models was not included in the scope of the evaluation and therefore should not 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 Protection Profiles 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.

4.1 TOE Description

The TOE is the FortiSandbox software 4.4 running on the FortiSandbox 500G, FortiSandbox 1500G, FortiSandbox 3000F or as a virtual appliance on VMware ESXI 8.0 (herein referred to as the TOE). TOE interfaces include an administrative CLI via direct serial connection or SSH and an administrative web GUI via HTTPS.

4.2 Evaluated Configuration

This evaluation covers the TOE only in its evaluated configuration. To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation identified in Section 6. When installed as a physical network appliance, the TOE evaluated configuration is a standalone network device. When installed as a virtual network appliance, the TOE evaluated configuration is a virtual network device.

The ST contains a list of evaluated models and firmware revisions applicable to those models. Details regarding the evaluated configuration are provided in Section 8 below.

4.3 TOE Physical Boundaries

As a standalone network appliance, the TOE consists of the following parts:

Hardware:

- FortiSandbox 1500G, using an AMD EPYC 7313P CPU on the Zen 3 microarchitecture
- FortiSandbox 500G, using an AMD EPYC 3251 CPU on the Zen microarchitecture
- FortiSandbox 3000F, using an AMD EPYC 7402 CPU on the Zen 2 microarchitecture

Software:

- FortiSandbox version 4.4.6-build 4527
- Included with the product, and available for download from the Fortinet website as a binary file.

As a virtual network appliance running on an ESXi virtualization server, the TOE consists of the following parts:

Software:

- The FortiSandbox 4.4.6-build 4527 (interim) VM image for ESXi virtualization servers

5 Security Policy

This section contains the product security features and services and contains the policies or rules that the TOE must comply with and/or enforce.

5.1 Security Audit

- The TOE will audit all events and information defined in Table 4: Auditable Events of the [ST].
- The TOE will also include the identity of the user that caused the event (if applicable), date and time of the event, type of event, and the outcome of the event.
- The TOE protects storage of audit information from unauthorized deletion
- The TOE prevents unauthorized modifications to the stored audit records.
- The TOE supports transmitting audit data to an external IT entity using TLS protocol.

5.2 Cryptographic Support

The TSF performs cryptographic operations as defined in the TSS Section 7.2. This includes:

- key generation for TLS and SSH using RSA, ECC, and FFC
  - RSA with key sizes of 2048 bits or greater
  - ECC over NIST curves P-256, P-384, and/or P-521
  - FFC using 2048-bit or greater keys in accordance with FIPS PUB 186-4
  - FFC using safe-primes according to NIST SP 800-56A r3
- key establishment in SSH and TLS sessions using ECDSA or DH/ECDH
  - ECC according to NIST SP 800-56A rev3
  - FFC according to FIPS PUB 186-4 and NIST SP 800-56A rev3
  - FFC using Safe Primes, according to NIST SP 800-56A
- bulk encryption using AES in CBC or GCM modes with 128 or 256 bit keys.
- Cryptographic signature generation and verification using RSA or ECDSA
  - RSA with modulus 2048-bit or greater according to FIPS PUB 186-4 Section 5.5
  - ECDSA over curves NIST P-256, P-384, and/or P-521, according to FIPS PUB 186-4 Section 6 and Appendix D
- Cryptographic hashing operations using SHA-1, SHA-2-256, SHA-2-384, and/or SHA-2-512
  - Keyed Hashing operations using the same underlying hashes in an HMAC function: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512

For details on the cryptographic operations performed by the TOE and the certificates which govern those operations, please see [ST] Section 7.2

The TSF zeroizes all plaintext secret and private cryptographic keys and CSPs once they are no longer required.

5.3 Identification and Authentication

The TSF supports passwords consisting of alphanumeric and special characters. The TSF also allows administrators to set a minimum password length and support passwords with 15 characters or more.

The TSF requires all administrative users to authenticate before allowing the user to perform any actions other than viewing the warning banner. The TOE may take certain automatic actions prior to authenticating any user:

- generating ephemeral session keys for SSH or TLS sessions, when any user attempts to connect.
- displaying the configured advisory and consent message, in accordance with the “Access Banner” requirement.

These TSF operations occur before identification and authentication.

5.4 Security Management

The TOE provides management functionality over both local and remote interfaces.

The local interface to a standalone hardware TOE is a dedicated physical port, which provides a direct console interface to the TOE's CLI.

Local access to a virtual TOE is through the ESXi console via URL.

For both standalone hardware TOEs and virtual TOEs, the remote interfaces are an SSH connection to the CLI and a web GUI accessed over TLS/HTTPS.

The TOE supports one default fully privileged user account, Admin, which corresponds to the PP defined Security Administrator. The Admin account has full privileges to all administrative functions.

The TOE supports an additional role: "TOE Users", who may be configured with none, some, or all of the permissions of a "Security Administrator". This enables administrators to delegate some or all of the tasks necessary to manage the TOE roles with lesser permissions. Collectively, all user accounts with administrative permissions are "administrators".

5.5 Protection of the TSF

The TSF prevents the reading of all pre-shared keys, symmetric keys, private keys, and plaintext-passwords.

The TOE provides reliable time stamps for itself.

The TOE runs a suite of self-tests during initial start-up (on power on), and when cryptographic operations are performed to demonstrate the correction operation of the TSF.

The TOE provides a means to verify firmware/software updates to the TOE using a digital signature mechanism prior to installing those updates.

5.6 TOE Access

The TOE, for local interactive sessions, terminates the session after an Authorized Administrator-specified period of session inactivity.

The TOE terminates a remote interactive session after an Authorized Administrator-configurable period of session inactivity.

The TOE allows Administrator-initiated termination of the Administrator's own interactive session.

Before establishing an administrative user session, the TOE displays a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.7 Trusted Path/Channels

The TOE is capable of using TLS to provide a trusted communication channel between itself and all authorized IT entities.

The TOE permits the TSF, or the authorized IT entities to initiate communication via the trusted channel.

The TOE is capable of using SSH or TLS/HTTPS to provide a communication path between itself and authorized remote Administrators.

The TOE permits remote administrators to initiate communication via the trusted path.

The TOE requires the use of the trusted path for initial administrator authentication and all remote administration actions.

6 Documentation

The following documents are provided with the product by the developer to the consumer and were evaluated along with the TOE:

- *FortiSandbox 4.4 NDcPP Common Criteria Technote*, 34-446-1080542-20251027, Thursday, October 30, 2025

- *FortiSandbox 4.4.6 Administration Guide*, 34-445-1030730-20240523, December 20, 2024
- *FortiSandbox 4.4.6 Getting Started*, 34-444-1011093-20250731, December 20, 2024
- *FortiSandbox 4.4.0-4.4.7 Install Guide for VMware*, 34-445-888478-20250221, February 21, 2025
- *FortiSandbox 4.4.0 Log Reference*, 34-440-922625-20230711, July 11, 2023

Any additional documentation provided with the product, or that is available online was not included in the scope of the evaluation and 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 documentation from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

The evaluation team configured the TOE according to the vendor-provided guidance documentation and performed the tests specified in the Supporting Documents (SD) for each PP These results are summarized in the evaluation Assurance Activity Report (AAR) with the approach summarized here.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities of this product.

7.2 Evaluation Team Independent Testing

The CCTL evaluation team created the test plan.

The functional testing was performed by CCTL evaluation team according to a Common Criteria Certification document and ran the tests specified in the NDcPP30e and PKG_SSH_V1.0, including tests associated with optional requirements. The CCTL evaluation team generated the Detailed Test Report using the evidence collected by the CCTL evaluation team during the testing.

7.3 Vulnerability Analysis

The evaluation team performed each AVA_VAN.1 CEM work unit (as refined by the SD) and each AVA_VAN evaluation activity defined in the SD. A vulnerability analysis was performed following the processes described in the PP. The vulnerability analysis included a public domain search for potential vulnerabilities. This search was performed on October 21, 2025, and no applicable vulnerabilities were discovered.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration consists of the following models:

Physical Models:

- FortiSandbox 1500G, using an AMD EPYC 7313P CPU on the Zen 3 microarchitecture
- FortiSandbox 500G, using an AMD EPYC 3251 CPU on the Zen microarchitecture
- FortiSandbox 3000F, using an AMD EPYC 7402 CPU on the Zen 2 microarchitecture

Virtual Models:

- FortiSandbox version 4.4.6-build 4527

8.2 Excluded Functionality

The following TOE Features are disabled by default and are excluded from the scope of this evaluation:

- HTTP GUI
- The TOE acting as a Telnet server
- The TOE acting as a TFTP client
- NTP

There are additional features available on the TOE that were not evaluated as part of this evaluation activity including:

- FortiGuard and FortiSandbox Community Cloud
- High Availability (Cluster)
- Use of syslog
- SMTP
- SNMP
- LDAP
- RADIUS
- Telnet
- TFTP
- Inline Block (HTTP2) (port 4443)
- ICAP (port 1344)
- ICAP/SSL (port 11344)

Consult the FortiSandbox 4.4 NDcPP Common Criteria Technote, 34-446-1080542 for additional information.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. The evaluation methodology used by the evaluation team to conduct the evaluation is the *Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5. The evaluation was successful and provides a level of assurance that the TOE meets the Security Functional Requirements identified in the Security Target. This assurance comes from the performance of the work units associated with the Security Assurance Requirements. A detailed description of those Assurance Requirements as well as the details of how the product meets each of them can be found in the Security Target. A more detailed account of the evaluation assurance activities and the results obtained can be found in the Assurance Activity Report.

9.1 Security Target Evaluation (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 TOE 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 target PPs.

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 was justified.

9.2 TOE Development (ADV)

The evaluation team applied each EAL 1 ADV CEM work unit as refined by the target PPs. This activity is considered implicitly resolved.

9.3 Guidance Documents (AGD)

The evaluation team applied each EAL 1 AGD CEM work units as refined by the target PPs. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the target PPs.

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's 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.

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

9.4 TOE Life Cycle Support (ALC)

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

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.

9.5 TOE Tests (ATE)

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 target PPs and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validation team 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 target PPs and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment (AVA)

The evaluation team applied each EAL 1 AVA CEM work unit as refined by the target PPs. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing, and did not discover any issues with the TOE. A list of search terms, databases searched, and evaluation findings may be found in the AVA. The evaluation team also performed additional Assurance Activities as required by the target PPs and documented that in the AAR

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the target PPs 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 *FortiSandbox 4.4 NDcPP Common Criteria Technote, 34-446-1080542-2025090520251027,* Thursday, October 30, 2025 and *FortiSandbox 4.4.6 Administration Guide, 34-445-1030730-20240523*, December 20, 2024. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. Evaluation activities are strictly bound by the assurance activities described in the NDcPP30e, PKG_SSH_V1.0, and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Security Target

The Security Target is: *FortiSandbox 4.4 Security Target*, version 1.6, October 30, 2025

12 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

[1] *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*, dated April 2017, Version 3.1 Revision 5, CCMB-2017-04-001.

[2] *Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components,* April 2017, Version 3.1, Revision 5, CCMB-2017-04-002.

[3] *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components*, April 2017, Version 3.1, Revision 5, CCMB-2017-04-003.

[4] *Common Methodology for Information Technology Security Evaluation – Evaluation methodology*, April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.

[5] *collaborative Protection Profile for Network Devices*, Version 3.0e, December 6, 2023

[6] *Functional Package for Secure Shell (SSH),* Version: 1.0, May 13, 2021

[7] *FortiSandbox 4.4 Security Target*, version 1.6, October 30, 2025

[8] *FortiSandbox 4.4 NDcPP Common Criteria Technote*, 34-446-1080542-20251027, Thursday, October 30, 2025

[9] *FortiSandbox 4.4.6 Administration Guide*, 34-445-1030730-20240523, December 20, 2024

[10] *FortiSandbox 4.4.6 Getting Started*, 34-444-1011093-20250731, December 20, 2024

[11] *FortiSandbox 4.4.0-4.4.7 Install Guide for VMware*, 34-445-888478-20250221, February 21, 2025

[12] *FortiSandbox 4.4.0 Log Reference*, 34-440-922625-20230711, July 11, 2023

[13] *Common Criteria Evaluation Technical Report*, UL15437480-ETR v1.2, October 28, 2025

[14] *Assurance Activity Report*, UL15437480-AARv1.3, October 30, 2025

[15] *Vulnerability Analysis*, UL15437480 AVA Rev. 1.3, 10/28/2025

[16] *FortiSandbox vND Test Verdicts*, UL15437480 vND Test Rev. 1.4, 10/30/25

[17] *FortiSandbox vND Test Annex 1 TLSS*, UL15437480 vND Test Annex 1 Rev. 1.4, 10/30/2025

[18] *FortiSandbox vND Test Annex 2 TLSC*, UL15437480 vND Test Annex 2 Rev. 1.4, 10/30/2025

[19] *FortiSandbox vND Test Annex 3 x509*, UL15437480 vND ATE Annex 3 Rev. 1.4, 10/30/2025

[20] *FortiSandbox vND Test Annex 4 SSH*, UL15437480 vND Test Annex 4 Rev. 1.4, 10/30/2025

[21] *FortiSandbox pND Test Verdicts*, UL15437480 ATE pND Rev. 1.5, 10/30/25

[22] *FortiSandbox pND Test Annex 1 TLSS*, UL15437480 Annex 1 pND Rev. 1.5, 10/30/2025

[23] *FortiSandbox pND Test Annex 2 TLSC*, UL15437480 Annex 2 pND Rev. 1.5, 10/30/2025

[24] *FortiSandbox pND Test Annex 3 x509*, UL15437480 Annex 3 pND Rev. 1.5, 10/30/2025

[25] *FortiSandbox pND Test Annex 4 SSH*, UL15437480 Annex 4 pND Rev. 1.5, 10/30/2025