National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

for the
Appgate SDP Client 6.4

Report Number:	**CCEVS-VR-VID11493-2025**
Dated:	**30 January 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

Jenn Dotson
Lori Sarem
Chris Thorpe
The MITRE Corporation

Jade Stewart
National Information Assurance Partnership

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

Executive Summary

This Validation Report (VR) documents assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of the Appgate Software Defined Perimeter (SDP) Client 6.4 provided by Appgate Cybersecurity, Inc. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government, and no warranty of the TOE is either expressed or implied.

The evaluation of the Appgate SPD Client 6.4 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in January 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Leidos. 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, 7 October 2021
- *Functional Packages for Transport Layer Security (TLS),* Version 1.1, March 1, 2019.

The TOE is Appgate SDP Client 6.4 (running on Windows 11 and macOS 14.4). 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 documented in the ETR and the Assurance Activities Report (AAR). The Validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The technical information included in this report was obtained from the *Appgate SPD Client 6.4 Security Target*, Version 1.0, 10 January 2025, and analysis performed by the Validation team.

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:

- 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 PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

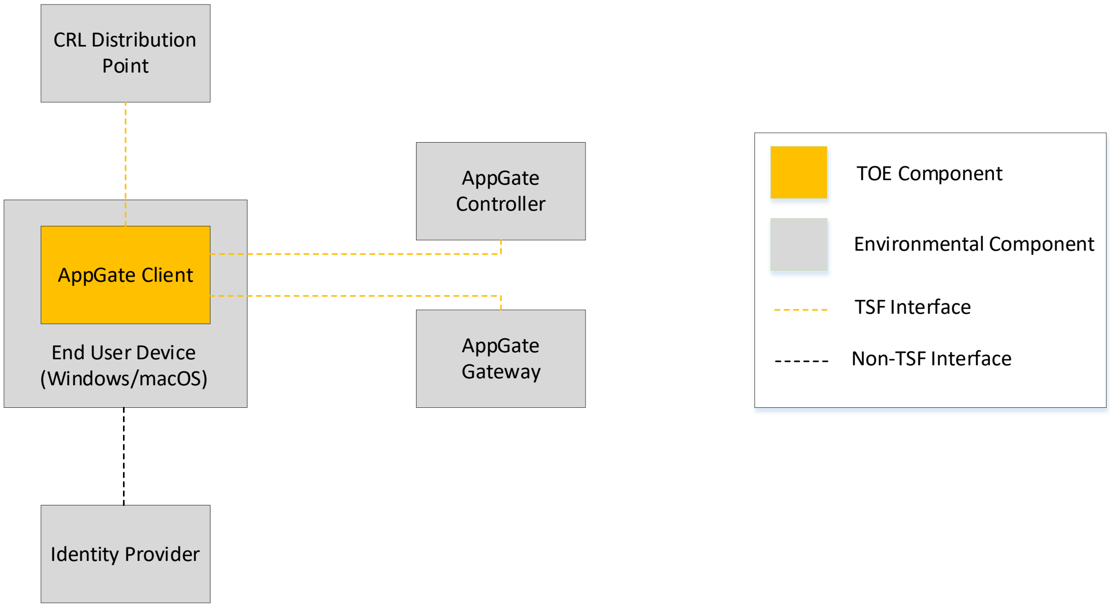
Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Appgate SDP Client 6.4
Security Target	*Appgate SDP Client 6.4 Security Target*, Version 1.0, January 10, 2025
Sponsor & Developer	Appgate Cybersecurity, Inc. 2 Alhambra Plaza, Suite PH-1-B Coral Gables FL, 33134
Completion Date	January 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	*Protection Profile for Application Software*, Version 1.4, 7 October 2021 and *Functional Package for Transport Layer Security (TLS)*, Version 1.1, March 1, 2019
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Dawn Campbell, Armin Najafabadi, Pascal Patin, Tony Apted
Validation Personnel	Jenn Dotson, Lori Sarem, Jade Stewart, Chris Thorpe

TOE Architecture

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

The Appgate Software Defined Perimeter (SDP) Client TOE consists of the Appgate SDP Client application. The TOE has both Windows and macOS platform versions. For both platform versions, the UI is written in Javascript using the React framework, business logic is written in C# using .NET, and the driver is written in C and Rust. Third-party components used by the TOE are either linked into the TOE binaries or exist as standalone DLLs, depending on the library.

The below figure shows an example Appgate SPD Client deployment. An Appgate deployment supports multiple Controllers and multiple Gateways but the interfaces to these are identical. A CRL distribution point is required to validate the revocation status of TLS server certificates presented by the Appgate Controller and Gateway components. An Identity Provider (IdP) is used to provide third-party verification of user identity (e.g. when accessing resources that require authentication). When an OIDC IdP is used, the TOE facilitates IdP interaction via browser redirection, so the actual interface to the IdP is performed by the underlying platform; the Client passes any assertion returned by the IdP to the Controller via its single interface with it. When an AD IdP is used, the Controller itself interfaces with the IdP for user identity verification.



Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the *Appgate SPD Client 6.4 Security Target*.

Cryptographic Support

The TOE implements cryptography to protect data in transit. For data in transit, the TOE implements TLS as a client. The TOE supports TLS connections both with and without mutual authentication.

The TOE implements all cryptography used for these functions using its own implementations of wolfCrypt with NIST-approved algorithms. The TOE's DRBG is seeded using entropy from the underlying OS platform.

For data at rest, the TOE relies on its operational environment to control access to stored credential data.

User Data Protection

The TOE relies on platform full disk encryption and credential storage mechanisms to protect sensitive data at rest.

The TOE relies on the network connectivity, credential repository, and log functions of its host OS platform. All uses of network connectivity are user-initiated.

Identification and Authentication

The TOE supports X.509 certificate validation as part of establishing TLS connections. The TOE implements functionality to support various certificate validity checking methods, including the checking of certificate revocation status using CRL. If the validity status of a certificate cannot be determined, the certificate will be rejected.

Security Management

The TOE itself and the configuration settings it uses are stored in locations recommended by the platform vendor. The TOE is launched by an authenticated OS user and runs in the session context of that user; there is no interface for a non-administrator to act as an administrator through separate authentication. When connecting to a Controller in the operational environment, the TOE receives a policy which may restrict the user to a subset of the available management functions. The TOE's primary management function is to add and remove the Controller-provided profiles and to configure behavior related to credential storage.

Privacy

The TOE does not have an interface to request or transmit requested PII from a user; PII is only transmitted over the network if initiated by the user.

Protection of the TSF

The TOE enforces various mechanisms to protect itself against unauthorized modification and use. The TOE implements address space layout randomization (ASLR), does not allocate any memory with both write and execute permissions, does not write user-modifiable files to directories that contain executable files, is compiled using stack overflow protection, and is compatible with the security features of its host OS platform.

The TOE contains libraries and invokes system APIs that are well-known and explicitly identified.

The TOE has a mechanism to determine its current software version. Software updates to the TOE are acquired through the application's connection to the Controller in the operational environment and subsequently applied using the TOE platform. All updates are digitally signed to guarantee their authenticity and integrity.

Trusted Path/Channels

The TOE encrypts sensitive data in transit between itself and its operational environment using TLS. These interfaces are used to secure all data in transit between the TOE and its operational environment.

Assumptions and Clarification of Scope

Assumptions

The Security Problem Definition, including the Assumptions, can be found in the following document:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021

That information has not been reproduced here, and the Application Software PP should be consulted if there is interest in that material.

Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the Application Software PP as described for this TOE in the ST. 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, with a certain level of assurance (the assurance activities specified in *Protection Profile for Application Software*, Version 1.4, 7 October 2021 and *Functional Packages for Transport Layer Security (TLS),* Version 1.1, March 1, 2019, was performed by the evaluation team).
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The TOE consists solely of software and relies on its operational environment for supporting security functionality, as identified in the ST.
- 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 Application Software PP and the TLS Functional Package. Any additional security related functional capabilities of the TOE were not covered by this evaluation. Specifically, TLS connectivity was tested in accordance with the Functional Package. The use of TLS functionality as a VPN was not evaluated.

Documentation

Appgate Cybersecurity, Inc., offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE are as follows:

- *Appgate SDP User Guide,* version 6.4, September 02, 2024
- *Appgate SDP Client 6.4 Common Criteria Evaluated Configuration Guide (CCECG),* Version 1.0, November 6, 2024

To use the product in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Appgate SDP Client 6.4 Common Criteria Test Report and Procedures for Application Software 1.4,* Version 1.1, January 23, 2025

A non-proprietary description of the tests performed, and their results are provided in the following document:

- *Assurance Activities Report for Appgate SDP Client 6.4*, Version 1.1, January 23, 2025

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST.

Developer Testing

The assurance activities do not specify any requirement for developer testing of the TOE.

Evaluation Team Independent Testing

The Evaluation team devised a Test Plan based on the Testing Assurance Activities specified in Protection Profile for Application Software and Functional Package for Transport Layer Security (TLS). The Test Plan described how each test activity was to be instantiated within the TOE test environment. The Evaluation team executed the tests specified in the Test Plan and documented the results in the team test report and AAR listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from 2 September 2024 to 15 November 2024.

The Evaluation team received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the guidance provided, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the Evaluation team, the testing requirements for Protection Profile for Application Software and Functional Package for Transport Layer Security (TLS), were fulfilled.

Test Configuration

The evaluation team established a test configuration consisting of the TOE (Appgate SDP Client 6.4) installed on each of the following devices:

- Dell Precision 3570 w/ Intel® Core™ i7-1255U, running Windows 11 23H2
- MacBook Pro w/ Apple M1 Max CPU, running Sonoma 14.4.1.

Testing environment:

- TLS Test Server: used for TLS client/server testing and port scanning.
- Revocation Test Server: used for CRL revocation responses .
- DNS Server: resolve DNS queries

- Appgate SDP Gateway/Controller appliances: Used to initiate a protected session with a remote resource.
- OIDC Identity Provider: Used to test the OIDC redirect method of authentication.

Evaluated Configuration

The TOE consists of the Appgate SDP Client version 6.4.2-39991 (for Windows) and version 6.4.2-40808 (for macOS) software application, that communicates only with the Appgate SDP appliance (Controller/Gateway), using TLS 1.2 provided by WolfSSL. The TOE is evaluated on Windows 11 and macOS 14.4 system. The TOE runs on the platform OS as a standalone component.

Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary *Evaluation Technical Report for Appgate SDP Client 6.4*. The reader of this document can assume that all assurance activities and work units received passing verdicts.

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, and the specific evaluation activities specified in *Protection Profile for Application Software*, Version 1.4, 7 October 2021, and *Functional Package for Transport Layer Security (TLS)*, Version 1.1, March 1, 2019. The evaluation determined the Appgate SDP Client 6.4 to be Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the Application Software PP and the TLS Functional Package.

Evaluation of the Security Target (ST) (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 Appgate SPD Client 6.4 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.

Evaluation of the Development (ADV)

The Evaluation team applied each ADV_FSP.1 CEM work unit. The Evaluation team assessed the evaluation evidence and found it adequate to aid in understanding how the TSF provides the security functions and meets the requirements specified in the claimed Protection Profile for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

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.

Evaluation of the Guidance Documents (AGD)

The Evaluation team performed each guidance assurance activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was 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.

Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit. The evaluation team ensured the TOE was labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

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.

Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team performed each test activity and applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the claimed PP and Functional Package and recorded the results in the 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.

Vulnerability Assessment Activity (AVA)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is contained in the AVA report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities.

The Evaluation team searched the National Vulnerability Database (https://nvd.nist.gov/) for vulnerabilities related to the TOE's operation. The Evaluation team used NVD's Basic and Advanced search features (https://nvd.nist.gov/vuln/search) and SNYK's Vulnerability Database (https://security.snyk.io/), to carry out the vulnerability searches. The final vulnerability search was conducted on 23 January 2025.

The Evaluation team also searched the following vendor specific Security Advisories forum for vulnerabilities related to the product/third-party libraries.

- Appgate- https://www.appgate.com/support/security-advisories
- WolfSSL- https://www.wolfssl.com/docs/security-vulnerabilities/
- Microsoft- https://msrc.microsoft.com/update-guide/vulnerability/

- Apple- https://support.apple.com/en-us/100100
- OpenSC- https://github.com/OpenSC/OpenSC/wiki/OpenSC-security-advisories

The Evaluation team used the following search terms in the searches of these repositories:

- "Appgate SDP Client 6.4" (TOE)
- “Appgate”(TOE)
- "Windows 11 23H2 10.0.22631.2506" (OE)
- "Apple macOS 14.4" (OE)
- The third-party libraries referenced in section 3.6.1 of the *Assurance Activities Report for Appgate SDP Client 6.4*, Version 1.1, January 23, 2025.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE.

The Appgate SPD Client 6.4 evaluation included the Vendor submission of a Software Bill of Materials (SBOM) for analysis, per NIAP policy. The SBOM provided a comprehensive listing of the third-party library components contained in the TOE. The SBOM was used in the vulnerability analysis during the evaluation period and was updated by the Vendor as requested by NIAP.

The conclusion drawn from the vulnerability analysis is that no residual TOE vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

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.

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.

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 *Appgate SDP User Guide,* version 6.4, September 02, 2024 and *Appgate SDP Client 6.4 Common Criteria Evaluated Configuration Guide (CCECG),* Version 1.0, November 6, 2024 listed in the Documentation section of this VR. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore, should not be relied upon to configure or operate the TOE as evaluated.

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST and only that functionality was evaluated. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness. Specifically, while TLS connectivity was evaluated in accordance with the Functional Package. The use of TLS for VPN functionality was not evaluated as there are no VPN requirements for TLS to evaluate against.

The Validation team strongly recommends that all TOE platforms in the operational environment are kept up to date with patches as they are released.

Security Target

The ST for this product's evaluation is *Appgate SDP Client 6.4 Security Target*, Version 1.0, January 10, 2025.

Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PII	Personally Identifiable Information
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

Bibliography

The validation team used the following documents to produce this VR:

[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 requirements, Version 3.1, Revision 5, April 2017.

[4] Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] Protection Profile for Application Software, Version 1.4, 7 October 2021.

[6] Functional Package for Transport Layer Security (TLS), Version 1.1, March 1, 2019.

[7] Appgate SDP Client 6.4 Security Target, Version 1.0, January 10 ,2025. (ST)

[8] Appgate SDP User Guide, version 6.4, September 02, 2024.

[9] Appgate SDP Client 6.4 Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, November 6, 2024. (AGD)

[10] Evaluation Technical Report for Appgate SDP Client 6.4 (Proprietary), Version 1.1, January 23, 2025. (ETR)

[11] Assurance Activities Report for Appgate SDP Client 6.4, Version 1.1, January 23, 2025. (AAR)

[12] Appgate SDP Client 6.4 Common Criteria Test Report and Procedures for Application Software 1.4, Version 1.1, January 23, 2025. (DTR)

[13] Appgate SDP Client 6.4 Vulnerability Analysis, Version 1.1, January 23, 2025. (AVA)