National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Ivanti Connect Secure 22.2

Report Number: CCEVS-VR-VID11372-2024
Dated: 02/23/2024
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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers
Marybeth Panock
Dave Thompson

The Aerospace Corporation

Russell Fink
Robert Wojcik

Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Reema Nagwekar
Calvin Sneed
Ruban Abinesh
Rahul Joshi

Intertek Acumen Security

Table of Contents

1 Executive Summary

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

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Ivanti Connect Secure 22.2 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in February 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. 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 2.2e, 27 March 2020 [PP-ND].

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Ivanti Connect Secure 22.2
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND]
Security Target	Ivanti Connect Secure 22.2 Security Target
Evaluation Technical Report	Evaluation Technical Report for Ivanti Connect Secure 22.2
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Ivanti, Inc. 10377 South Jordan Gateway, Suite 110 South Jordan, Utah 84095
Developer	Ivanti, Inc. 10377 South Jordan Gateway, Suite 110 South Jordan, Utah 84095
Common Criteria Testing Lab (CCTL)	Intertek Acumen Security Rockville, MD
CCEVS Validators	Jerome Myers, Dave Thompson, Marybeth Panock, Russell Fink, Robert Wojcik

3 Architectural Information

3.1 Product Type

Ivanti Connect Secure enables secure device access to applications and resources in the data center and in the cloud. This clientless system provides unified management of policies, compliance, and authorizations for cloud and data center access. The single sign-on and Layer 3 SSL VPN functionality of the Product are outside the scope of this evaluation. For a list of product features and functionality that is excluded from the evaluation, please refer to Section **Error! Reference source not found.** of the Ivanti Connect Secure 22.2 Security Target [ST].

3.2 TOE Usage

The TOE is classified as a network device (a generic infrastructure device that can be connected to a network) or a virtual network device (a Virtual Appliance that can be connected to a network) depending on the underlying platform. The TOE software consists of Ivanti Connect Secure (ICS) 22.2R3. The appliance's software is built on IVE OS 3.0. The TOE consists of the ICS application, IVE OS, and either the TOE hardware or the VM hypervisor, all of which are delivered with the TOE. The TOE hardware consists of either the ISA Models 6000, 8000C, or 8000F.

The TOE provides following security features that are part of the evaluated configuration:

- Secure remote administration of the TOE via HTTPS/TLS web interface
- Secure Local administration of the TOE
- Secure connectivity with remote audit servers using mutually authenticated TLS
- Identification and authentication of the administrator of the TOE
- CAVP validated cryptographic algorithms
- Self-protection mechanisms such as executing self-tests to verify correct operation
- Secure firmware updates

For a complete list of security features provided by the TOE, please refer to Section 1.3.2 of Ivanti Connect Secure 22.2 Security Target [ST].

4 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v2.2e or NDcPP.

4.1 Security Audit

The TOE generates audit records for security relevant events. The TOE maintains a local audit log and can send audit records to a remote Syslog server. Audit records sent to the remote server are protected by a TLS connection. Each audit record includes identity (username, IP address, or process), date and time of the event, type of event, and the outcome of the event. The TOE prevents modification to the local audit log.

4.2 Cryptographic Support

The TOE includes the Ivanti Secure Cryptographic Module that implements CAVP-validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. These algorithms are used to provide security for the TLS and HTTPs connections for secure management and secure connections to a syslog server. TLS and HTTPs are also used to verify firmware updates. The cryptographic services provided by the TOE are described below.

Table 1 TOE Cryptographic Protocols

Cryptographic Protocol	Use within the TOE
TLS (client)	Secure connection to syslog FCS_TLSC_EXT.1, FCS_TLSC_EXT.2
HTTPS/TLS (server)	Secure management connections and verification of firmware updates via web browser FCS_HTTPS_EXT.1, FCS_TLSS_EXT.1
AES	Provides encryption/decryption in support of the TLS protocol. FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1
DRBG	Deterministic random bit generation used to generate keys. FCS_TLSS_EXT.1, FCS_RBG_EXT.1
Secure hash	Used as part of digital signatures and for hashing passwords prior to storage on the TOE. FCS_COP.1/Hash, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1,FPT_APW_EXT.1
HMAC	Provides keyed hashing services in support of TLS. FCS_COP.1/KeyedHash, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1
ECDSA	Provides key generation and signature generation and verification in support of TLS. FCS_CKM.1, FCS_COP.1/SigGen, FCS_COP.1/SigVer, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1
EC-DH	Provides key establishment for TLS. FCS_CKM.2, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1
RSA	Provide key generation and signature generation and verification (PKCS1_V1.5) in support of TLS. FCS_CKM.1, FCS_COP.1/SigGen, FCS_COP.1/SigVer, FCS_TLSC_EXT.1,FCS_TLSC_EXT.2, FCS_TLSS_EXT.1

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified in Section 6.1 CAVP Algorithm Certificate Details in Ivanti Connect Secure 22.2 Security Target [ST].

4.3 Identification and Authentication

The TOE authenticates administrative users using a username/password or username/X.509 certificatecombination. The TOE does not allow access to any administrative functions prior to successful authentication. The TOE validates and authenticates X.509 certificates for all certificate uses.

The TOE supports passwords consisting of alphanumeric and special characters and enforces minimumpassword lengths. The TSF supports certificates using RSA or ECDSA signature algorithms. The TOE only allows users to view the login warning banner and send/receive ICMP packets prior toauthentication. Remote administrators are locked out after a configurable number of unsuccessful authenticationattempts.

4.4 Security Management

The TOE allows users with the Security Administrator role to administer the TOE over a remote web UIor a local CLI. These interfaces do not allow the Security Administrator to execute arbitrary commandsor executables on the TOE. Security Administrators can manage connections to an external Syslog server, as well as determine the size of local audit storage.

4.5 Protection of the TSF

The TOE implements several self-protection mechanisms. It does not provide an interface for the reading of secret or private keys. The TOE ensures timestamps, timeouts, and certificate checks are accurate by maintaining a real-time clock. Upon startup, the TOE runs a suite of self-tests to verify that itis operating correctly. The TOE also verifies the integrity and authenticity of firmware updates by verifying a digital signature of the update prior to installing it.

4.6 TOE Access

The TOE can be configured to display a warning and consent banner when an administrator attempts toestablish an interactive session over the local CLI or remote web UI. The TOE also enforces a configurable inactivity timeout for remote and local administrative sessions.

4.7 Trusted Path/Channels

The TOE uses TLS to provide a trusted communication channel between itself and remote Syslog servers.The trusted channels utilize X.509 certificates to perform mutual authentication. The TOE initiates the TLS trusted channel with the remote server.

The TOE uses HTTPS/TLS to provide a trusted path between itself and remote administrative users. TheTOE does not implement any additional methods of remote administration. The remote administrativeusers are responsible for initiating the trusted path when they wish to communicate with the TOE.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

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

Table 2- Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protectedin its operational environment and not subject to physicalattacks that compromise the security or interfere with thedevice's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionalityas its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, nonon-TOE guest VMs are allowed on the platform.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the deviceitself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

ID	Assumption
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATION	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.

ID	Assumption
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

5.2 Threats

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

Table 3 - Threats

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrativesession, or sessions between Network Devices. Successfully gaining Administrator access allows maliciousactions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithmsor 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 takeadvantage 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.
ID	**Threat**
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 the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

5.3 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND]
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that the evaluators discover while performing the work units.
- Consistent with NIAP requirements, the evaluators searched publicly available databases to identify known vulnerabilities. Any that were found to be relevant to the product at the time of the completion of the evaluation have been mitigated.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality described in Section 7.2 of this report is not covered by the scope of the evaluation.

6 Documentation

The following guidance documents constitute the administrator guidance provided by the vendor for configuring and operating the TOE in its evaluated configuration.

- Ivanti Connect Secure 22.2 Common Criteria Configuration Guide v1.2 [AGD]

This is the only document that should be trusted for use when installing or administering the product in its evaluated configuration.

This document is available from the NIAP Product Compliance List (PCL) entry for this product.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

This section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references.

The TOE consists of the hardware identified in Section 7.1.1 running Ivanti Connect Secure (ICS) v22.2R3, when configured in accordance with the documentation identified in Section 6.

In the below diagram, the TOE consists of the appliance within the blue line. Everything else is not included within the TOE and is part of the TOE environment.

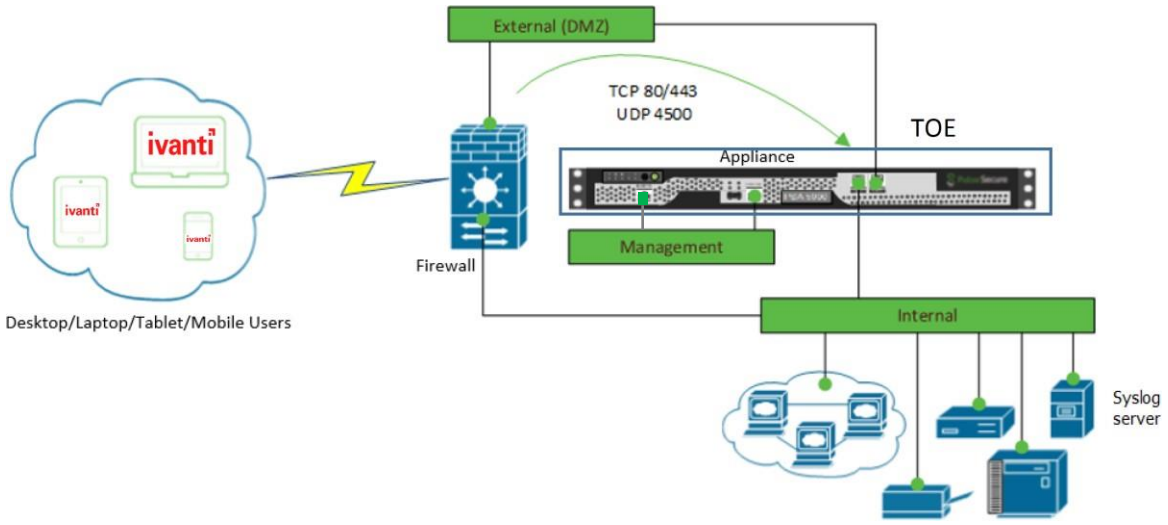

Figure 1 – Representative TOE Deployment

7.1.1 Physical Boundaries

The TOE consists of the following hardware:

- ISA 6000
- ISA 8000C
- ISA 8000F

Running:

- Ivanti Connect Secure (ICS) v22.2R3

The TOE can also be a virtual appliance (ISA-V) on VMware ESXi 6.7, with a Dell PowerEdge R640 as thehardware platform. The ICS software runs on any of the TOE hardware appliance platforms or on a virtual appliance. The TOE is delivered with the ICS v22.2R3 software installed on one of the ISA appliances. The platforms provide different amounts of processing power and network connectivityoptions as described in Table 4.

Table 4 – TOE Hardware Details

Model	Processor	Network Options
ISA 6000	Intel Core i3 10100E 10th gen(Comet Lake)	2 x 10 Gigabit Copper Ethernet traffic ports 1 x 1GbE Management port 1 x RJ-45 Console Port
ISA 8000C	Intel Xeon Gold 5317 (Ice Lake)	2 x 10 Gigabit Ethernet copper traffic ports with link redundancy 1 x 1GbE Management port 1 x RJ-45 Console Port
ISA 8000F	Intel Xeon Gold 5317 (Ice Lake)	2 x 10 Gigabit fiber trafficports with link redundancy 1 x 1GbE Management port 1 x RJ-45 Console Port

The TOE can also be a virtual appliance on VMware ESXi 6.7, with a Dell PowerEdge R640 as the hardwareplatform. ESXi is a bare-metal hypervisor so there is no underlying operation system. In the evaluated configuration, there are no guest VMs on the physical platform providing non-network device functionality. The virtual appliance platform is described below.

The virtual appliance can be download by customers from https://my.pulsesecure.net/ and installed on compliant hardware listed below. License are provided by Ivanti Secure via email. When a customer request is received, Ivanti will provide an authcode via email. Customers must register in https://my.pulsesecure.net portal and generate the license string by providing Hardware id with earlier provided authcode. These auth codes are not reusable.

Table 5 - VMware Host Details

Model	Processor	Hypervisor
ISA-V (virtual platform) onPowerEdge R640	Intel(R) Xeon(R) Gold 6252 CPU @2.10GHz	VMware ESXi 6.7

7.2 Excluded Functionality

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

- Layer 3 SSL VPN
- Application VPN
- Endpoint Integrity and Assessment
- Layer 7 Web single sign-on (SSO) via SAML
- Mobile Device Management Integration

These features may be used in the evaluated configuration; however, no assurance as to the correct operation of these features is provided.

The TOE includes the following functionality that is not covered in this Security Target and may not be enabled or used in the CC evaluated configuration:

- DMI Agent
- SNMP Traps

External Authentication Servers for administrator authentication

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the ETR for Ivanti Connect Secure 22.2, which is not publicly available. However, the AAR provides an overview of the testing and the tools that were used for testing in Section 4, test cases in Sections 5 and 6, and the prescribed assurance activities in Section 7.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

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 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 Rev. 5 and CEM version 3.1 Rev. 5. The evaluation determined the Ivanti Connect Secure 22.2 to be Part 2 extended compliant, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Ivanti Connect Secure 22.2 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND].

The validator reviewed the work of the evaluation team and found that it provided sufficient evidence and justification to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND].

related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that it provided sufficient evidence and justification to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the

evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND] related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team and found that it provided sufficient evidence and justification confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

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

The validator reviewed the work of the evaluation team and found that it provided sufficient evidence and justification to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND] and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team and found that it provided sufficient evidence that the evaluation activities addressed the test activities in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND], and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The search criteria, the date of the search, and a summary of the results can be found in the Assurance Activity Report [AAR], Section 7.6. The vulnerability search was last conducted on 6 Feb 2024.

The validator reviewed the work of the evaluation team and found that it provided sufficient evidence and justification to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND], and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

No versions of the TOE, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target [ST]. Other functionality included in the product was not assessed as part of this evaluation.

Note that the Administrator Guidance [AGD], Section 7.2.1 describes audit records that indicate the start-up and shutdown of the Audit Functions. These audit records more precisely describe the start-up and shutdown of the Remote Audit Functions. The Local Audit Functions should continue to perform auditing even when remote auditing is shut down.

All other concerns and issues are adequately addressed in other parts of this document.

11 Security Target

The Ivanti Connect Secure 22.2 Security Target v0.6 [ST] and the other public documents are available on the NIAP web page associated with this product's entry in the Product Compliant List (see https://www.niap-ccevs.org/Product/index.cfm).

12 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

This Validation Report is based on the following criteria and evaluation reports:

[CC-P1] *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model,* Version 3.1 Revision 5, Apr 2017.

[CC-P2] *Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements,* Version 3.1 Revision 5, Apr 2017.

[CC-P3] *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements*, Version 3.1 Revision 5, Apr 2017.

[CEM] *Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5, Apr 2017.

[PP-ND] *Collaborative Protection Profile for Network Devices,* Version 2.2e, 27 Mar 2020

[ST] *Ivanti Connect Secure 22.2 Security Target*, v0.6, 12 Dec 2023

[AAR] *Assurance Activity Report for Ivanti Connect Secure 22.2,* v1.2, 6 Feb 2024

[AGD] *Ivanti Connect Secure v22.2 Common Criteria Configuration Guide,* v1.2, 1 Feb 2024

[AVA] *Vulnerability Assessment for Ivanti Connect Secure*, v1.3, 16 Feb 2024.

[ETR] *Evaluation Technical Report for Ivanti Connect Secure 22.2* v1.1, 15 Dec 2023

[ISA6] *Test Plan for Ivanti Connect Secure ISA 6000*, v1.1, 14 Dec 2023

[ISA8] *Test Plan for Ivanti Connect Secure ISA 8000*, v1.1, 12 Dec 2023

[ISAV] *Test Plan for Ivanti Connect Secure ISA-V*, v1.1, 20 Nov 2023