National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

™

Validation Report

for the

Ivanti Policy Secure 22.7R1

Report Number: CCEVS-VR-VID11565-2025

Dated: 06/27/2025

Version: 1.0

National Institute of Standards and Technology	**Department of Defense**
Information Technology Laboratory	**ATTN: NIAP, SUITE: 6982**
100 Bureau Drive	**9800 Savage Road**
Gaithersburg, MD 20899	**Fort George G. Meade, MD 20755-6982**

ACKNOWLEDGEMENTS

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 Policy Secure 22.7R1 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 Intertek Acumen Security in June 2025. 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 3.0e, 06 December 2023.

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 Policy Secure 22.7R1
Protection Profile	Collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023
Security Target	Ivanti Policy Secure 22.7R1 Security Target, version 1.4
Evaluation Technical Report	Evaluation Technical Report for Ivanti Policy Secure 22.7R1, version 0.8
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Ivanti, Inc.
Developer	Ivanti, Inc.
Common Criteria Testing Lab (CCTL)	Intertek Acumen Security, 2400 Research Blvd Suite 395 Rockville, MD 20850
CCEVS Validators	Daniel Faigin Marybeth Panock

3 Architectural Information

3.1 TOE Type

Ivanti Policy Secure (IPS) is a next-generation Network Access Control (NAC) that enables visibility to understand an organization's security posture and enforce role-based access and endpoint security policies for network users. IPS allows administrators to define, implement, and enforce policy by enabling endpoint discovery, monitoring, and alerting. For a list of product features and functionality that is excluded from the evaluation, please refer to Section 1.5 [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 Policy Secure (IPS) 22.7R1. The appliance's software is built on IVE OS 3.0. The TOE includes the IPS application and the IVE OS, along with the underlying platform, which may be either be dedicated TOE hardware or a virtualized environment managed by a VM hypervisor, all of which are delivered with the TOE. The TOE hardware includes either the ISA Models 6000, 8000C, or 8000F. In the case of a virtual deployment, the TOE includes the IPS application and the IVE OS running within a virtual machine that is hosted on the hypervisor.

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 via a serial console connection
- 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

4 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E], hereafter referred to as NDcPP v3.0e or NDcPP.

4.1 Security Audit

The TOE generates audit records for security relevant events. The TOE maintains a local audit log and also sends the audit records to a remote Syslog server as soon as they are generated, in real-time. 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. The TSF manages local audit storage using two log files (active and inactive). When the active log file reaches its capacity, the TSF overwrites the inactive log file (if it exists). If no inactive log file is available, the TOE creates a new log file, switches logging to the new file, and generates an audit log indicating the capacity limit was reached.

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 alsoused 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
HTTPS/TLS (client)	Secure connection to syslog FCS_HTTPS_EXT.1, 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 establishment, key generation, signature generation and verification (PKCS1_V1.5) in support of TLS. FCS_CKM.1, FCS_CKM.2, 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' [ST].

4.3   Identification and Authentication

The TOE authenticates administrative users using a username/password or username/X.509 certificate combination. 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 minimum password 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 GUI or a local CLI. These interfaces do not allow the Security Administrator to execute arbitrary commands or executables on the TOE. Security Administrators can manage connections to an external Syslog server, as well as determine the size of local audit storage.

9

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 it is 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 to establish 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. The TOE does not implement any additional methods of remote administration. The remote administrative users 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 protected in its operational environment and not subject to physical attacks that compromise the security or cPP_ND_v3.0e, 06-Dec-2023 41 interfere with the device'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 functionality as 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, no non-TOE guest VMs are allowed on the platform

ID	Assumption
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 device itself, 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).
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.

ID	Assumption
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.
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 administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them

ID	Threat
	unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Nonvalidated 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. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
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

ID	Threat
	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 3.0e, 06 December 2023 [CPP_ND_V3.0E].

- 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 is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6   Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Ivanti Policy Secure 22.7R1 Security Target, version 1.4
- Ivanti Policy Secure 22.7R1 Common Criteria Configuration Guide, version 0.6

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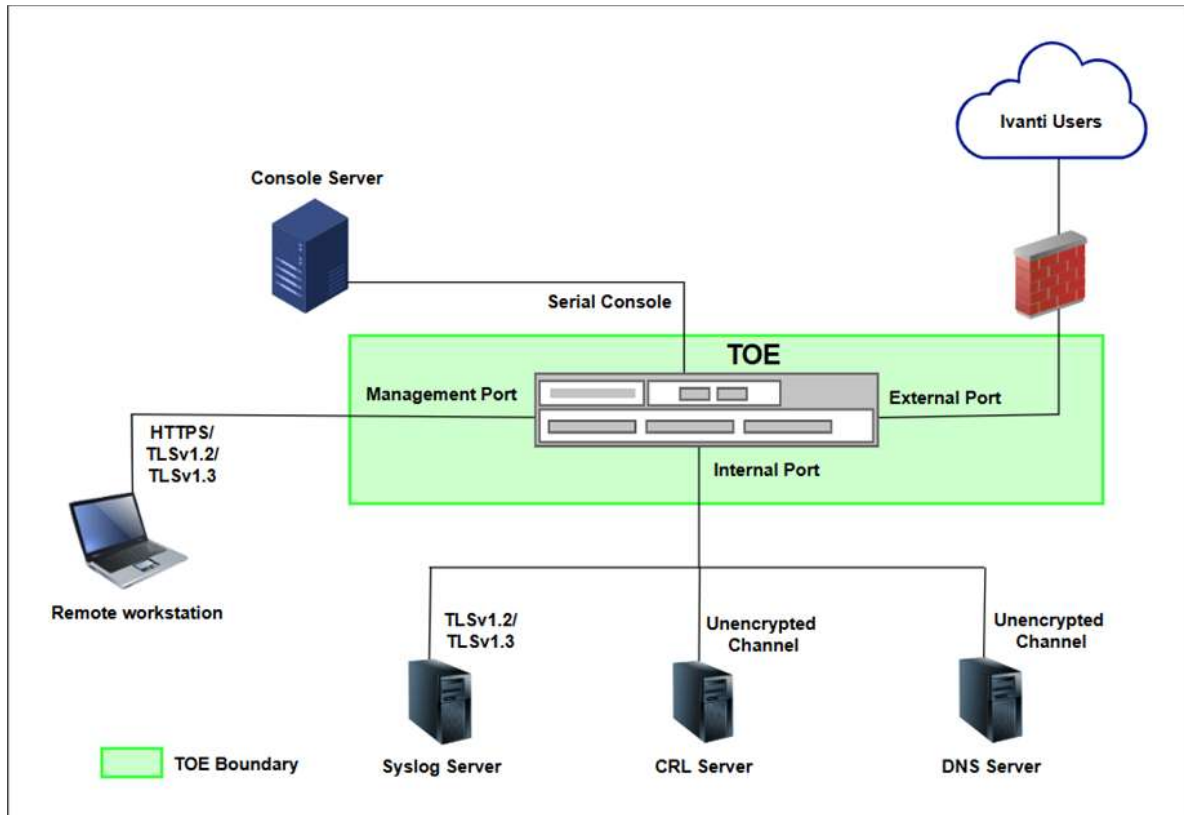

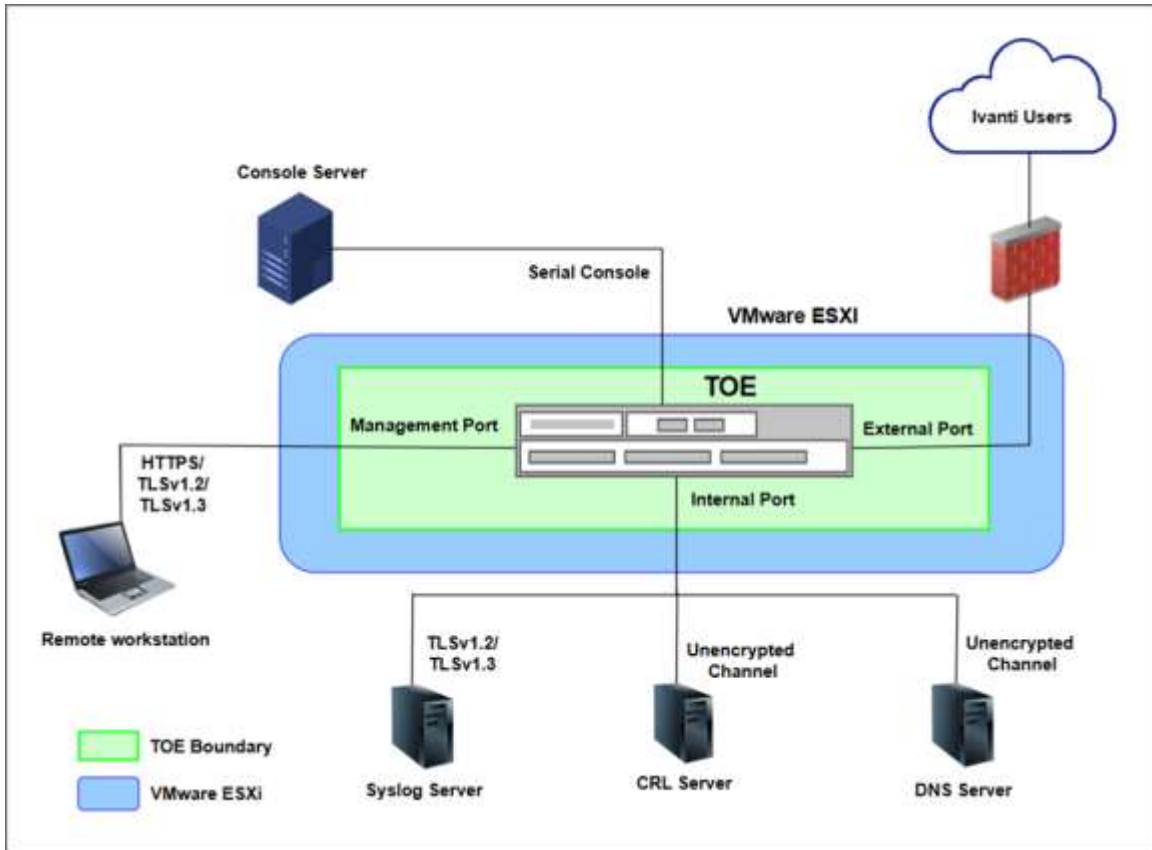**Figure 1– Representative TOE Deployment of Physical Appliance**

Figure 2 – Representative TOE Deployment of Virtual Appliance

The TOE consists of the following hardware:

- ISA 6000
- ISA 8000C
- ISA 8000F

Running:

- Ivanti Policy Secure (IPS) v22.7R1

These platforms run Ivanti Policy Secure (IPS) 22.7R1. The IPS software is delivered pre-installed on one of the above hardware appliances. The TOE is delivered with the IPS v22.7R1 software installed on one of the ISA appliances. The platforms provide different amounts of processing power and network connectivity options as described in Table 4 – TOE Physical Boundary Components.

Table 4 – TOE Physical Boundary Components

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 traffic ports with link redundancy 1 x 1GbE Management port 1 x RJ-45 Console Port

The TOE can also be a virtual appliance hosted on VMware ESXi 8.0.3, with a Dell PowerEdge R640 powered by an Intel(R) Xeon(R) Gold 6252 (Cascade lake) as the hardware platform. ESXi is a bare-metal hypervisor so there is no underlying operation system. In the evaluated configuration, there are no guest VMs on the hypervisor providing non-network device functionality. The virtual appliance platform is described in Table 5 - Virtual TOE Models.

Customers can obtain the virtual appliance by contacting Ivanti Support through https://forums.ivanti.com/s/contactsupport?language=en_US. To access the software, customers need to register on the support portal and follow the required process. Please note that authcodes are single-use and cannot be reused. The appliance should be installed on compliant hardware as listed below.

Table 5 - Virtual TOE Models

Model	Processor	Hypervisor
ISA 6000-V (virtual platform) on PowerEdge R640	Intel(R) Xeon(R) Gold 6252 (Cascade lake)	VMware ESXi 8.0.3
ISA 8000-V (virtual platform) on PowerEdge R640	Intel(R) Xeon(R) Gold 6252 (Cascade lake)	VMware ESXi 8.0.3

7.1.1 TOE Environment

The following environmental components are required to operate the TOE in the evaluated configuration:

Table 6 – Required Environmental Components

Components	Description
Syslog server	• Conformant with RFC 5424 (Syslog Protocol).

Components	Description
	• Supporting Syslog over TLS (RFC 5425). • Acting as a TLSv1.3 and/or TLSv1.2 server. • Supporting Client Certificate authentication.
Remote workstation	• Provides remote management of TOE. • Microsoft Edge 101, Google Chrome 102, or Firefox 100. • Supporting TLSv1.3 and/or TLSv1.2. • Allows direct uploads of software image files via the TOE's GUI.
CRL Server	• Provides CRLs through CRL Distribution Points in certificates. • Uses HTTP protocol for CRL distribution to clients. • Conformant with RFC 5280.
DNS Server	• Translates a Fully qualified domain name (FQDN) into IP addresses for network communication. • Uses UDP and TCP protocols on port 53. • Conformant with RFC 1035.
Console Server	• Provides local access to the console port of network device. • A null modem crossover cable is connected from the console terminal to the device's serial port.
VMware ESXi	• Hosts the virtualized TOE. • Supports hardware virtualization and resource allocation (CPU, memory, storage).

7.2 Excluded Functionality

The following product functionalities are not included in the CC evaluation:

- Network Security and Application Access Control Integration
- Federation
- Guest Access
- Anti-Malware Protection and Patch Assessment
- Firewall Listening Service
- IPv6 protocol support

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
- REST API
- External Authentication Servers for administrator authentication
- Full Disk Encryption

These functionalities are disabled by default, and no administrator configuration is required.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for Ivanti Policy Secure 22.7R1, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

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 3.0e, 06 December 2023 [CPP_ND_V3.0E]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8.3 Testing Location

All testing was carried out at the Acumen Security office located at 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from October 2024 to June 2025. Although there may be evaluators working remotely accessing the testing environment over a VPN, the TOE is located at the lab in the US and under the CCTL's control.

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept in a secure repository.

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 TOE Name to be Part 2 extended, 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 Policy Secure 22.7R1, 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 3.0e, 06 December 2023 [CPP_ND_V3.0E].

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

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 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 3.0e, 06 December 2023 [CPP_ND_V3.0E], 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 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.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 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 3.0e, 06 December 2023 [CPP_ND_V3.0E], 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 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 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 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 sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

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 collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E], 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 sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities on 06/17/2025, performed vulnerability testing and did not discover any issues or open vulnerabilities with the TOE.

The validator 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 addressed the

vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E], 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 3.0e, 06 December 2023 [CPP_ND_V3.0E], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the guidance documents listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Specifically, note the Excluded Functionality, described in Section 7.2.

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

11 Annexes

Not applicable.

12 Security Target

Ivanti Policy Secure 22.7R1 Security Target, version 1.4

13 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.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.

2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.

3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.

4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.

5. collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023

6. Ivanti Policy Secure 22.7R1 Security Target, version 1.4, June 26, 2025 (ST)

7. Assurance Activity Report for Ivanti Policy Secure 22.7R1, version 1.7, June 26, 2025 (AAR)

8. Evaluation Technical Report for Ivanti Policy Secure 22.7R1, Version 0.8, June 26, 2025 (ETR)

9. Ivanti Policy Secure 22.7R1 Common Criteria Configuration Guide, Version: 0.6, June 20, 2025 (AGD)

10. Vulnerability Assessment for Ivanti Policy Secure 22.7R1, Version: 0.5, June 17, 2025 (AVA)

11. Test Plan for Ivanti Policy Secure 22.7R1 ISA 6000, version 1.1, June 20, 2025 (DTR)

12. Test Plan for Ivanti Policy Secure 22.7R1 ISA 8000-V, version 1.1, June 20, 2025 (DTR)

13. Test Plan for Ivanti Policy Secure 22.7R1 ISA 6000C, version 1.1, June 20, 2025 (DTR)