Agenzia per la Cybersicurezza Nazionale

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 11/23

(Certificate No.)

Prodotto: Ivanti Security Controls 2022.2 (Version 9.5.9293.0)

(Product)

Sviluppato da: Ivanti

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+
(ALC_FLR.2)

p. il Direttore Generale
dell'ACN

Il Capo Servizio
Certificazione e Vigilanza
(Andrea Billet)

[ORIGINAL SIGNED]

Roma, 14 novembre 2023

This page is intentionally left blank

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Ivanti Security Controls 2022.2 (Version 9.5.9293.0)

OCSI/CERT/CCL/06/2022/RC

Version 1.0

14 November 2023

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	14/11/2023

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM Decreto del Presidente del Consiglio dei Ministri

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza

NIS Nota Informativa dello Schema

OCSI Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

cPP collaborative Protection Profile

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

PP Protection Profile

SAR Security Assurance Requirement

SFP Security Functional Policy

SFR Security Functional Requirement

SOGIS Senior Officials Group Information Systems Security

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

3.3 Other acronyms

API Application Programming Interface

CVE Common Vulnerabilities and Exposures

FIPS Federal Information Processing Standard

GUI	Graphical User Interface
ID	Identifier
OS	Operating System
SQL	Structured Query Language

4 References

4.1 Normative references and national scheme documents

[CC1] CCMB-2017-04-001, "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, "Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components", Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, "Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components", Version 3.1, Revision 5, April 2017

[CCRA] "Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security", July 2014

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

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 Agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 Agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 Agosto 2023

[SOGIS] "Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", Version 3, January 2010

4.2 Technical documents

[ETR1] Evaluation Technical Report, Ivanti Security Controls 2022.2, IVANTI-025_v3, CCLab Software Laboratory, 30 August 2023

[ETR2] Evaluation Technical Report Ivanti Security Controls 2022.2, IVANTI-025_v4, CCLab Software Laboratory, 19 October 2023[AGD] Ivanti Security Controls 2022.2 Guidance Documentation Supplement, version: 0.10, 11 August 2023

[ST] Ivanti Security Controls 2022.2 Security Target, version: 0.11, 7 November 2023

5 Recognition of the certificate

5.1 European Recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA for all declared assurance components.

5.2 International Recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 8 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all declared assurance components.

6 Statement of certification

The Target of Evaluation (TOE) is the product “Ivanti Security Controls 2022.2 (Version 9.5.9293.0)”.

The TOE is an integrated software solution providing patch management, asset inventory, IT administration, and reporting functionality. These functions are supported through the Security Controls application.

Based on the provided functionality, the TOE type is identified as “Other Devices and Systems”. The TOE is a Windows-based software solution that is comprised of the following components:

- Security Controls Console.
- Security Controls Agent.
- Security Controls Deployment Tool Chain.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should also review the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL2, augmented with ALC_FLR.2, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product "Ivanti Security Controls 2022.2 (Version 9.5.9293.0)" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Ivanti Security Controls 2022.2 (Version 9.5.9293.0)
Security Target	Ivanti Security Controls 2022.2 Security Target, version: 0.11, 7 November 2023
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.2
Developer	Ivanti
Sponsor	Corsec Security, Inc.
LVS	CCLab Software Laboratory - Budapest Site
CC version	3.1 Rev. 5
PP conformance claim	No conformance claimed
Evaluation starting date	10 March 2022
Evaluation ending date	30 August 2023

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE is an integrated software solution providing patch management, asset inventory, IT administration, and reporting functionality. These functions are supported through the Security Controls application.

The TOE is a Windows-based software solution that is comprised of the following components:

- Security Controls Console.
- Security Controls Agent.

- Security Controls Deployment Tool Chain.

The Security Controls Console is the hub of all scanning, deployment, scheduling and reporting tasks. A TOE user must have Windows login credentials with administrative access to the host OS. Functions available are based on the role assigned. The Security Controls Console supports both agent-based and agentless endpoint administration. An agentless configuration is where no persistent software is required on the managed endpoint. Agentless operations are all executed and controlled through the Security Controls Console. Agentless scans are performed to determine the health of machines on the network. Other agentless operations include patch deployment and remote IT Script execution.

The Security Controls Agent is installed on a managed endpoint to support policy-based administration. The Security Controls Agent operates autonomously according to a policy provided by the Security Controls Console, that is created by a TOE user with the Administrator role. This option provides flexibility to overcome network topology challenges such as interrupted connectivity. A policy is a set of operating rules defining what a Security Controls Agent will do. The policy is used by the Security Controls Agent to determine the patch health of the host machine. Based on the health, patches are deployed according to the rules in the policy. Security Controls Agents may get patch updates directly from the Security Controls Console, from a Distribution Server, or from vendor web sites.

Agentless systems are managed remotely by the Security Controls Console. Patch deployment on agentless systems is handled through the Security Controls Deployment Tool Chain. The Security Controls Deployment Tool Chain is pushed by the Security Controls Console to the specified agentless machines. This tool facilitates patch execution, scheduling, and status reporting. To perform scheduled operations, the Security Controls Deployment Tool Chain includes the Security Controls Scheduler service. The Security Controls Scheduler can be remotely managed from the Security Controls Console using the Scheduled Tasks Manager application. The Security Controls Scheduler will be installed on demand when a scheduled operation is requested.

7.3.1 TOE architecture

Figure 1 shows the logical scope of the TOE and TOE boundaries.

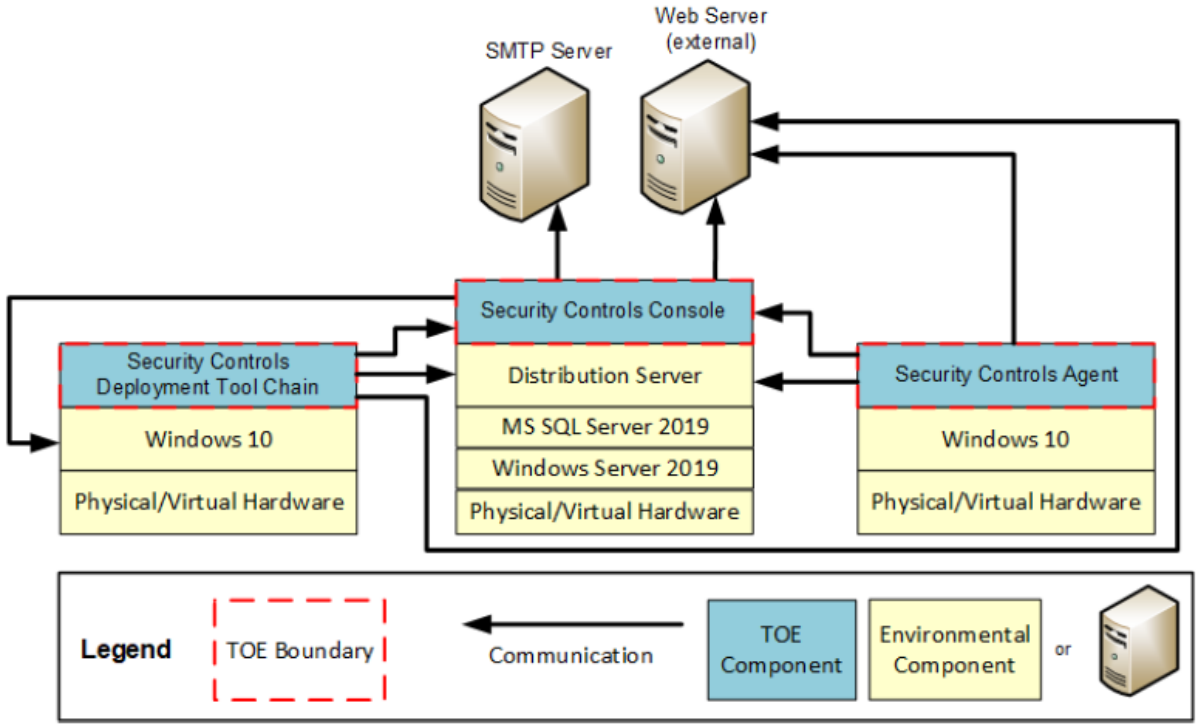

Figure 1 - TOE logical scope and boundaries

The TOE can be divided into the following subsystems:

- Security Controls Console.
- Security Controls Agent.
- Security Controls Deployment Tool Chain.

The Security Controls Console is the server component of the TOE. The Security Controls Console is a Windows-based application that is installed on Windows Server 2019. The Security Controls Console is composed of the Security Controls Console GUI, services and Patch Engine components. The GUI provides a front-end interface to users. The core patch scanning and deployment logic is implemented in the Patch Engine. The Security Controls Console also contains a Windows Service host for various Security Controls Console services including Results Import, Agent Support/STS, Deploy Monitor, Data Sync, Scheduler, IT Script Engine, REST API, and Hypervisor Patch.

Distribution Servers can be used in an agent-based or agentless scenario to reduce the impact of patch deployment on the network. A Distribution Server is a local cache of patches available for installation. Patches are stored on a configured Distribution Server (a server with a network file share). The Distribution Server can be the Security Controls Console machine's patch repository or any other network file share. (For the purposes of this evaluation, the Distribution Server is located on the same machine as the Security Controls Console).

The Security Controls Agent is an agent service that is installed on a physical or virtual machine connected to the network.

The agent-based configuration is an autonomous service installed on selected target machines.

The Security Controls Deployment Tool Chain allows agentless machine targets to patch safely.

The Security Controls Scheduler is a piece of the Security Controls Deployment Tool Chain that schedules patch deployment and allows staging of future deployments.

Agentless and agent-based configurations may be used together ensuring networks are effectively managed while remote users' applications are secure and up to date on patches.

For a detailed description of the TOE, consult the section 1.5 of Security Target [ST].

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in section 3 of the Security Target [ST].

The TOE security functions are described in detail in section 7 of the Security Target [ST]. The most significant aspects are summarized below:

- **Security Audit**: the TOE generates audit records each time a machine is scanned, a patch is applied, and a security violation is discovered. It also allows an authorized user to review the audit records. Audit records are also generated on startup and shutdown of the application, but these audit events are stored in the Windows Event Logs. An authorized user may view the Windows Event Logs through the Windows Event Viewer. Functionality associated with the Windows Event Logs is outside the scope of this evaluation and will not be covered in this Certification Report.

- **User Data Protection**: the TOE implements an Access Control Security Functional Policy (SFP), which mediates access to the TOE's security functions. The TOE also implements an information flow control SFP, called Protect SFP, which mediates access to machine-scanning functionality and patch-deployment functionality.

  The TOE imports end user application patch binaries from vendor websites. When applicable, certificate validation is performed before the information is allowed into the TOE. This validation uses the Windows OS FIPS 140-2 validated Cryptographic Service Provider. If the binaries cannot be validated, then they are not downloaded into the TOE (the Windows OS FIPS 140-2 validated Cryptographic Service Provider is outside the scope of the evaluation).

  The TOE exports end user application patch binaries to the Distribution Server. An authenticated user with appropriate access identifies end user application patch binaries. The files are exported from the TOE to the specified Distribution Server where they will be retrieved by the agentless and agent-based target machines during the patch deployment process.

- **Identification and Authentication**: the TOE maintains the unique Windows user account identifier (ID) and assigns a role for each user for access control and auditing purposes.

- **Security Management**: the TOE provides following security management functions, upon which Access Control and Protect Control are enforced:

  - Management of security functions behaviour.

- Management of security attributes.
- Management of TSF data.

The TOE authorizes access to security functions and attributes based on the user's Windows OS login credentials. (The Windows OS authentication functionality is not a part of this evaluation and will not be covered in this Certification Report). These credentials are used to identify the user's role and what information is available to be created, modified, and deleted.

- **Protection of the TSF**: Ivanti executables, patch data, and configuration data are protected from modification while being transmitted between separate parts of the TOE. Ivanti executables, TOE patch data, and configuration data are only distributed if the integrity of the data is determined to be valid. The integrity of TOE software is verified upon execution of a TOE component. The TOE component will only allow itself to execute or be executed by appropriately verified software. Integrity checking is based on digital signatures attached to Ivanti executable code, TOE patch data code, and configuration data. The cryptographic functionality related to generating and verifying digital signatures takes place in the Windows OS using a FIPS 140-2 validated Cryptographic Service Provider. (The Windows OS FIPS 140-2 validated Cryptographic Service Provider is outside the scope of this evaluation and will not be discussed further in this Certification Report).

- **Resource Utilization**: the TOE implements resource utilization mechanisms when performing patch scans, asset scans, and patch deployments. These engines are multithreaded, which means they may run multiple tasks at one time. When called, a number is passed defining how many threads (at maximum) are to be utilized simultaneously. Security Controls can attempt to scan up to 64 machines per CPU core simultaneously, with the default being 8 per CPU core. For example, on a 16-core system up to 128 machines can be scanned simultaneously by default.

- **Data Collection**: the TOE utilizes patch and asset scans to collect data about machines within the network. Patch scans provide updated detail on the health of a machine or machines in a machine group. Asset scans provide information about the hardware and software of physical and virtual machines. Scans on a machine or machine group are executed by an authorized user from the Security Controls Console GUI. If allowed in the agent policy, scans can also be executed by an authorized user on the local machine running the Security Controls Agent. This scan data is collected from the specified target machines, sent to the SQL database, and viewed from the Security Controls Console. Only authorized users may leverage this information to analyse the state of the network and determine key IT tasks to be performed.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage of the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

The ST includes the following extended functional requirements:

- **FDC_ANA_EXT.1**: This component is a member of a new family (FDC_ANA_EXT – System Analysis) which does not exist in CC Part 2 classes. FDC_ANA_EXT.1 is described as following: it provides the capability to analyse collected data and present the results to users in a way that easily allows them to respond to potential security violations found during the analysis.

- **FDC_SCN_EXT.1**: This component is a member of a new family (FDC_SCN_EXT: System Scan) which does not exist in CC Part 2 classes. FDC_SCN_EXT.1 is described as follow: it defines the scanning function and specifies which machines will have a scan performed on them.

- **FDC_STG_EXT.1**: This component is a member of a new family (FDC_STG_EXT - Scanned Data Storage) which does not exist in CC Part 2 classes. FDC_STG_EXT.1 is described as follow: it defines how the TSF protects stored scan data from unauthorized modification or deletion.

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory (Budapest Site).

The evaluation was completed on 30 August 2023 with the issuance by LVS of the Evaluation Technical Report [ETR1], which was approved by the Certification Body on 20 September 2023.

An additional ETR ([ETR2]) was delivered on 20 October 2023 including editorial changes.
Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR1] issued by the LVS CCLab Software Laboratory (Budapest Site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Ivanti Security Controls 2022.2 (Version 9.5.9293.0)" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2, augmented with ALC_FLR.2, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2, augmented with ALC_FLR.2.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
ST introduction	ASE_INT.1	Pass
Conformance claims	ASE_CCL.1	Pass
Security problem definition	ASE_SPD.1	Pass
Security objectives	ASE_OBJ.2	Pass
Extended components definition	ASE_ECD.1	Pass
Derived security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	*Pass*
Test	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass

Assurance classes and components		Verdict
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product "Ivanti Security Controls 2022.2 (Version 9.5.9293.0)" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Organizational Security Policies and the Assumptions described, respectively, in section 3.2 and 3.3 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE [AGD].

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The TOE software can be downloaded from the Ivanti website: https://forums.ivanti.com/s/article/Ivanti-Security-Controls-Common-Criteria-Certified-Download . There is another link (the "Direct download") from where the TOE can also be obtained: https://application.ivanti.com/isec/v9.5/installers/IvantiSecurityControls_2022.2.exe . The Security Controls Common Criteria Certified Download Page is available only to Ivanti customers with a valid Ivanti Community account. A link to download the certified version of the software can be found on this page. The Direct download link is publicly accessible if the URL is known, and the TOE software may be downloaded without registering an account.

After the software is downloaded, a one-time trial license activation can be enabled. Customers must purchase a full license by contacting Ivanti's Sales team who will then email the full license to the customer after the purchase. All documentation is available in the full license installation package as well as online at the below link and is included: https://www.ivanti.com/support/product-documentation .

9.2 Installation, initialization, and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the following documents contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST]:

- Ivanti Security Controls 2022.2 Guidance Documentation Supplement, version: 0.10, 11 August 2023 [AGD].

9.3 Identification of the TOE

Customers can verify the integrity of the Security Controls binaries by comparing the SHA-256 hash of the downloaded file to the hash provided on the TOE download page. Customers can view the file properties of Security Controls binaries to verify that they have the correct version. Users can also find instructions on how to confirm they are running the correct version in the "Getting Started" section of *Welcome to Ivanti Security Controls*.

Moreover, users can view the version visiting *About Security Controls* in *Help menu*.

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product "Ivanti Security Controls 2022.2 (Version 9.5.9293.0)", developed by Ivanti. The Evaluator followed the preparation steps defined in the [AGD] section 2.2 Secure Installation section for the TOE being in the evaluated configuration.

The following items must be available before performing the installation:

- TOE environment:
    - Security Controls Console hardware:
        - Microsoft Windows Server 2019 (excluding Server Core):
            - Microsoft Windows OS FIPS 140-2 validated Cryptographic Service Provider.
            - Microsoft Windows OS Event Log and Windows OS Event Viewer.
        - Microsoft SQL Server 2019.
        - Microsoft Visual C++ Redistributable 2015-2019.
        - Microsoft .NET Framework 4.8 or later.
    - Security Controls Agent hardware:
        - Microsoft Windows 10:
            - Microsoft Windows OS FIPS 140-2 validated Cryptographic Service Provider.
    - Security Controls Deployment Tool Chain hardware:
        - Microsoft Windows 10:
            - Microsoft Windows OS FIPS 140-2 validated Cryptographic Service Provider.
    - SMTP Server.
    - Cables, connectors, and switching and routing devices necessary for TOE communications with environmental components and the Internet including the Ivanti Web Server.
- TOE software:
    - Security Controls 2022.2.
- Guidance documentation [AGD].

The following features and functionality are included in the TOE by default and cannot be disabled. These features have not been tested against Common Criteria standard, and usage of these features is

considered to be outside of the scope of the evaluation. These features can be accessed only by a trusted administrator, who is assumed to be competent, non-hostile, appropriately trained, and follows all guidance.

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Third-party application control.
- PowerShell ITScripts customization.
- Security Controls Cloud features.
- Power Management features.
- Importing CVEs.
- Ivanti Application Control.

The following user roles are excluded from the evaluated configuration:

- Application Control report only.
- Patch and Application Control deploy and report.

For more details, please refer to sections 1.4.1,1.4.2 and 1.5.3 of the Security Target [ST].

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL2, augmented with ALC_FLR.2, such activities include the following three steps:

- Evaluation of the tests performed by the Developer in terms of coverage.
- Execution of independent functional tests by the Evaluators.
- Execution of penetration tests by the Evaluators.

11.1 Test configuration

For the execution of test activities, a test environment was set up at the LVS site.

The Evaluator was presented with a configuration identical to the one described in the [ST]. All TOE components were in the same LAN during testing, the Evaluator used Windows 10 as a general-purpose computer. One Windows 10 hosted the Security Controls Deployment Tool Chain. The Security Controls Agent was operated both on this and on another Windows 10 while the Security Controls Console was on one Windows Server 2019 Datacenter.

The Evaluator verified the system configuration according to the documentation provided by the developer [AGD] and the test documentation. The Evaluator then concluded that the test configuration is consistent with the [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer used a testing approach that resulted in covering all of the TSFIs with at least one test case. These test cases contain all the information required, e.g., prerequisites, step-by-step guide, expected and actual results.

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFRs) and the TSFIs described in the functional specification.

11.2.3 Test results

All test results from the tested environment show that the Developer's actual results were consistent with the expected results.

11.3 Functional and independent tests performed by the Evaluators

The Evaluator's sampling approach was selecting 3 test cases from 19 of test cases created by the Developer for which all steps were executed.

The following test cases were conducted by the Evaluator:

- Security Roles.
- Management of Security Attributes (user roles).

- Audit Review.

Conducting the test cases, the Evaluator was able to properly determine the behaviours of the TOE's Security Controls Console, Security Controls Agent and Security Controls Deployment Tool Chain. According to the testing activities, the Developer's expected and actual results were in line with the operation of the TOE.

Three tests (Evaluator Test Case 1 – Role deletion, Evaluator Test Case 2 – Usage of a Custom column and Filter Editor, Evaluator Test Case 3 – Google related patch scan) for the GUI of the Security Controls were generated for testing the role deletion, the usage of a Custom column and Filter Editor and the Google related patch scan because these were not tested using the Developer tests. The actual results were in line with the expected results in case of each test case.

All tests passed successfully.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same TOE sample already used for the functional test activities, verifying that the test configuration was consistent with the version of the TOE under evaluation.

The Evaluator executed some Nmap scans to find vulnerable service related to the TOE. No relevant service was identified and for the TOE and its components. According to these, the Evaluator found that the TOE had no vulnerable service, i.e., based on sources of information publicly available, there were no identified potential vulnerabilities in the TOE.

After a focused search of the Developer documentation, no potential vulnerabilities were found either.

There were 5 potential vulnerabilities analysed by the Evaluator:

- SQL injection.
- Log injection.
- Command injection.
- Bypass of authentication.
- Unencrypted communication.

Based on the available information, at the end of the evaluation, the Evaluator did not identify residual vulnerabilities, i.e., vulnerabilities that could be exploited only by an attacker with attack potential beyond Basic.