KECS-CR-25-41

AutoPassword Enterprise v4

Certification Report

Certification No.: KECS-CISS-1378-2024

2025. 12. 05.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2025.12.05.	-	Certification report for AutoPassword Enterprise v4 - First documentation

This document is the certification report for AutoPassword Enterprise v4 of eSTORM Co,. Ltd.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KoSyAs)

Table of Contents

1. Executive Summary

This report describes the evaluation result drawn by the evaluation facility on the results of the AutoPassword Enterprise v4 developed by eSTORM CO., Ltd. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (hereinafter referred to as “TOE”) is an Out-of-Band (OOB) server authentication product. When a user accesses an online service provided by a business server, instead of using the traditional password entry method, the TOE utilizes the user's mobile device to provide secure mutual authentication between the business server and the user.

The Target of Evaluation (hereinafter referred to as “TOE”) is an Out-of-Band (OOB) server authentication product. When a user accesses an online service provided by a business server, instead of using the traditional password entry method, the TOE utilizes the user's mobile device to provide secure mutual authentication between the business server and the user.

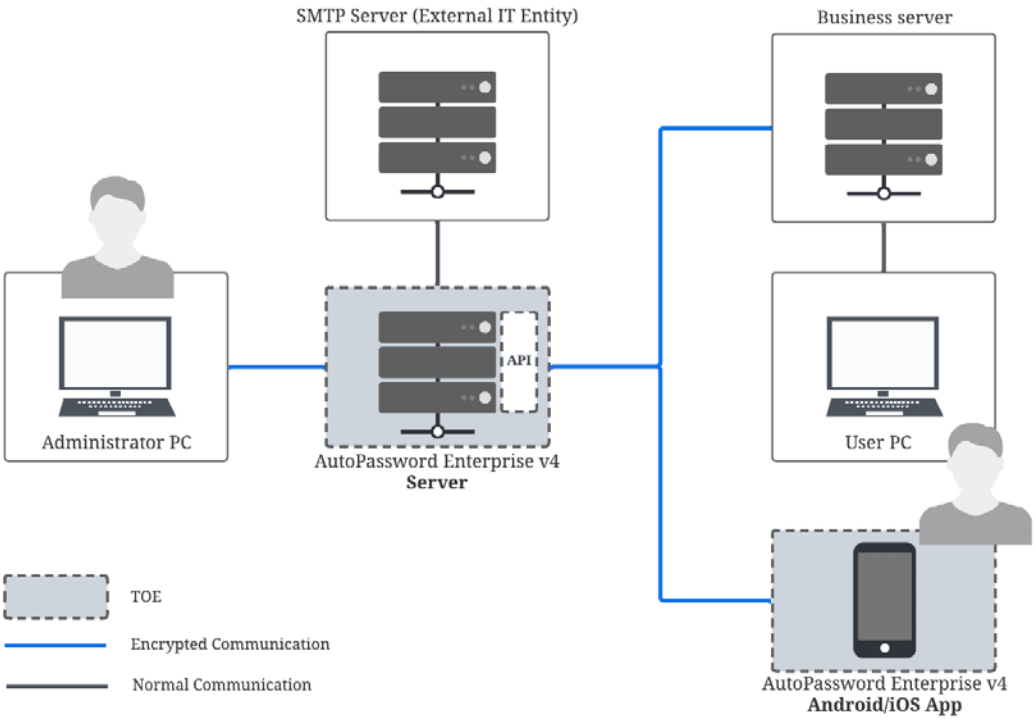
This system operates by first verifying the business server through an OOB channel using the AutoPassword Enterprise v4 Android, AutoPassword Enterprise v4 iOS App (hereafter "the authentication app") installed on the user's mobile device. This helps protect users from threats like phishing attacks and ensures they connect to a trusted online service.

Also, the TOE shall provide a variety of security features: security audit, cryptographic support, the user identification and authentication including mutual authentication between TOE components, security management, the TOE access session management, and the TSF protection function, etc.

The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on November 27, 2025. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted [6] and the Security Target (ST) [4].

The ST has no conformance claim to the protection profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of evaluation assurance level (EAL) 1. Therefore, the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and newly defined components in the Extended

Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.
[Figure 1] is a general operating environment. The TOE consists of the AutoPassword Enterprise v4 Server and the AutoPassword Enterprise v4 Android App, AutoPassword Enterprise v4 iOS App.



[Figure 1] TOE operational environment

TOE's authentication process flows as follows:

1) Server authentication: When a user attempts to log into the business server's online service, the business server presents the user with server authentication information generated by the AutoPassword Enterprise v4 Server, rather than requesting a password.
2) Comparison and verification: The user compares the server authentication information presented by the business server with the server authentication information independently generated by the authentication app on their mobile device.
3) Server trust confirmation: If the two pieces of information match, the user confirms the authenticity of the business server and approves the connection through the authentication app.
4) User authentication: Once server authentication is complete, the

authentication app generates user authentication information and sends it to the AutoPassword Enterprise v4 Server to complete the user's authentication.

5) Service provision: After the business server receives the authentication result from the AutoPassword Enterprise v4 Server, it provides the online service to the user

From an administrator's PC with an allowed IP address, the administrator accesses the AutoPassword Enterprise v4 Server's web management console via a web browser. After identification and authentication, they perform various security management tasks.

The user connects to the business server from a user's PC. During the authentication process, mutual authentication is performed by verifying the server authentication information and user authentication information, which are generated by the AutoPassword Enterprise v4 Server and the AutoPassword Enterprise v4 Android App, AutoPassword Enterprise v4 iOS App, respectively.

The business server's online service is provided to user requests after authentication is complete. The SMTP server (an external IT entity) performs the function of sending alarm emails when a potential security violation is detected.

The requirements for hardware, software and operating system to install the TOE are shown in [Table 1].

Component			Requirement
AutoPassword Enterprise v4 Server	HW	CPU	Intel(R) Core(TM) i5-13400 CPU @ 2.50 GHz or higher
		Memory	16 GB or higher
		HDD	10 GB or more of space required for TOE installation
		NIC	100/1000 Mbps * 1 EA or higher
	SW	OS	Rocky Linux 8.10(64 bit, kernel 4.18.0)
		WAS	Tomcat 9.0.111 NGINX 1.28.0
		JDK	OpenJDK 21.0.9_10
		DBMS	MariaDB 10.11.14
AutoPassword Enterprise v4	HW	Product Name	Samsung Galaxy S23

Android App		Model Number	SM-S911N
	SW	OS	Android 16(kernel 5.14.41)
AutoPassword Enterprise v4 iOS App	HW	Product Name	iPhone 13
		Model Number	MLQ73KH/A
	SW	OS	iOS 18(kernel 24.5.0)

[Table 1] TOE Hardware and Software specifications

External IT Entity	Description
Mail Server	It is used to send information mail to administrator in case of potential security threat of the TOE

[Table 2] External IT Entity

The 3rd party S/W Included in TOE is as follws.

Component	3rd party S/W	Description
AutoPassword Enterprise v4 Server	OpenSSL 3.0.18	TSF data encryption, communication channel encryption
AutoPassword Enterprise v4 Andoird App		
AutoPassword Enterprise v4 iOS App		

[Table 3] The 3rd party S/W included in TOE

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE reference is identified as follows.

Cls.	Contents
TOE	AutoPassword Enterprise v4
TOE Version	v4.0.3
TOE Component	AutoPassword Enterprise v4 Server v4.0.1 (autopassword_enterprise_v4_server_v4.0.1.tgz)
	AutoPassword Enterprise v4 Android App v4.0.1 (autopassword_enterprise_v4_android_app_v4.0.1.apk)
	AutoPassword Enterprise v4 iOS App v4.0.1 (autopassword_enterprise_v4_ios_app_v4.0.1.ipa)
Guidance document	AutoPassword Enterprise v4 Installation Manual v1.1 (AutoPassword Enterprise v4 Installation Manual v1.1.pdf)
	AutoPassword Enterprise v4 User Manual v1.1 (AutoPassword Enterprise v4 User Manual v1.1.pdf)

[Table 4] TOE identification

[Table 5] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea IT Security Evaluation and Certification Guidelines (Ministry of Science and ICT Guidance No. 2022-61) Korea IT Security Evaluation and Certification Regulation (Ministry of Science and ICT·ITSCC, May 17, 2021)
TOE	AutoPassword Enterprise v4
Common Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1 - Part 1: Introduction and general model, CC:2022 R1(CCMB-2022-11-001, 2022.11.) - Part 2: Security functional components, CC:2022 R1(CCMB-2022-11-002, 2022.11.) - Part 3: Security assurance components, CC:2022 R1(CCMB-2022-11-003, 2022.11.) - Part 4: Framework for the specification of evaluation methods

	and activities, CC:2022 R1(CCMB-2022-11-004, 2022.11.) - Part 5: Pre-defined packages of security requirements, CC:2022 R1(CCMB-2022-11-005, 2022.11.) - Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, CCMB-2024-07-002, 2024.7.
EAL	EAL1
Developer	eSTORM Co., Ltd.
Sponsor	eSTORM Co., Ltd.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	November 27, 2025

[Table 5] Additional identification information

3. Security Policy

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) [3]

4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the chapter 3.1 of ST [3])

- The TOE must be in a physically safe environment, and protected from unauthorized physical accesses.
- The authorized administrators of the TOE should not be malicious, and should be properly trained and perform their duties accurately according to administrator guidelines.
- The authorized administrator of the TOE shall ensure the reliability and security of the operating system by performing the reinforcement work on the latest vulnerabilities of the operating system in which the TOE is installed and operated.

Furthermore, some aspects of threats, and organizational security policies are not fulfilled by the TOE itself, thus these aspects are addressed by the TOE environment. Details can be found in the chapter 3.1 and 3.2 of ST [3]

This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. (for the detailed information of TOE version and TOE Components version refer to the [Table 4])

The scope of this evaluation is limited to the functionality and assurance covered in the Security Target.

This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. (for the detailed information of TOE version and TOE Components version refer to the [Table 4])

5. Architectural Information

1. Physical Scope of TOE

The physical scope of the TOE consists of the AutoPassword v4 Server, AutoPassword Enterprise v4 Android App, AutoPassword Enterprise v4 iOS App and Guidance document.

Hardware and OS where the TOE is installed are not included in the scope of the TOE.

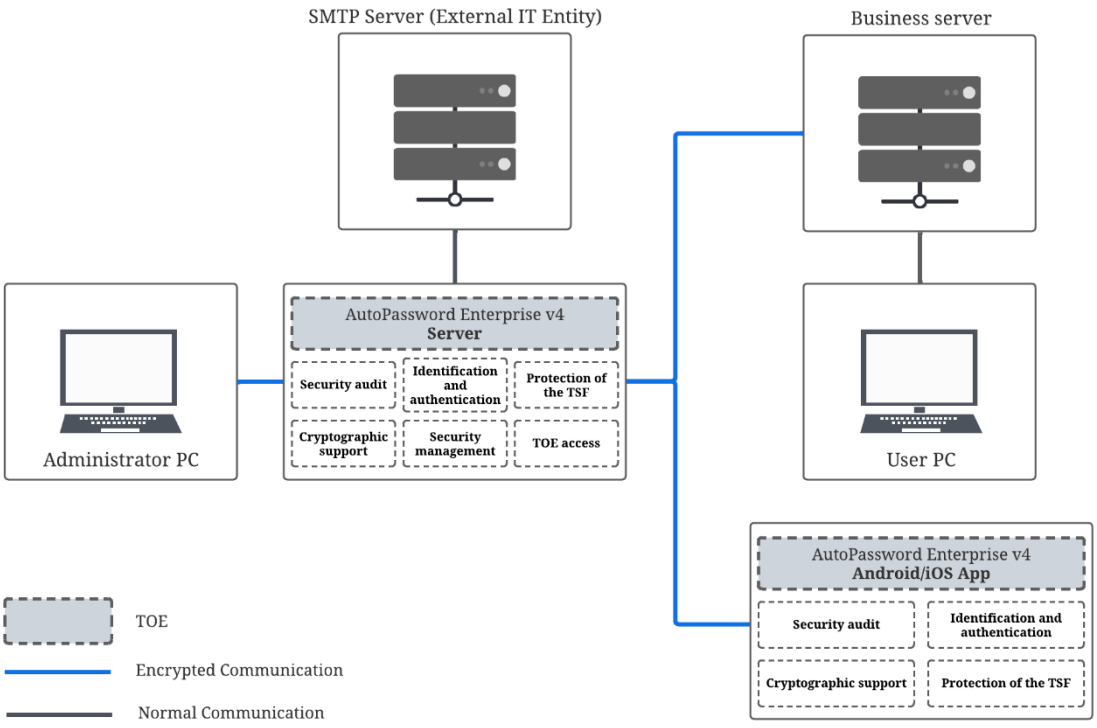
Category		Type	Delivery
TOE	AutoPassword Enterprise v4	-	-
TOE Version	v4.0.3	-	-

TOE Component	AutoPassword Enterprise v4 Server v4.0.1 (autopassword_enterprise_v4_server_v4.0.1.tgz)	S/W	Included in an installation CD of the product package provided to users
	AutoPassword Enterprise v4 Android App v4.0.1 (autopassword_enterprise_v4_android_app_v4.0.1.apk)	S/W	
	AutoPassword Enterprise v4 iOS App v4.0.1 (autopassword_enterprise_v4_ios_app_v4.0.1.ipa)	S/W	
Guidance Document	AutoPassword Enterprise v4 Installation Manual v1.1 (AutoPassword Enterprise v4 Installation Manual v1.1.pdf)	PDF	
	AutoPassword Enterprise v4 User Manual v1.1 (AutoPassword Enterprise v4 User Manual v1.1.pdf)		

[Table 6] Physical scope of TOE

2. Logical Scope of TOE

The logical scope of the TOE is as in [Figure 3] below.



[Figure 1] TOE Logical scope

▣ Security Audit (FAU)

The AutoPassword Enterprise v4 Server is designed to identify and record security-related events, enabling real-time detection of potential security violations and facilitating an effective response.

When situations like reaching the allowed number of authentication failures, self-test failures, integrity violations, or anticipated audit data loss occur, they are considered potential security violations. An alarm email is immediately sent to the administrator in these cases.

When an event occurs, the server automatically generates an audit record that includes the event's date and time, type, outcome (success or failure), and the subject's identity.

Generated audit records are provided in a user-friendly format. The authorized administrator can query and sort the audit data based on criteria such as keywords, date ranges, and event types.

Audit data is stored securely in an internal DBMS. An alarm email is sent to the administrator once each time the storage usage exceeds 60%, 70%, and 80% of its total allocated capacity.

When the storage is full, the oldest audit records are automatically overwritten. In this event, an alarm email is also sent to the administrator, allowing them to be aware of potential data loss in advance.

AutoPassword Enterprise v4 Android App, AutoPassword Enterprise v4 iOS App identifies auditable events, such as identification and authentication, self-tests, and integrity verification, and transmits the audit data to the AutoPassword Enterprise v4 Server to be recorded.

▣ Cryptographic support (FCS)

The AutoPassword Enterprise v4 Server provides various cryptographic functions based on standard technologies to encrypt communication channels between TOE components, protect server and user authentication information, protect sessions, and ensure the confidentiality and integrity of important stored data. These functions are implemented through proven cryptographic algorithms and secure key management procedures, covering the entire lifecycle of cryptographic keys from generation to destruction.

Cryptographic key generation is performed as follows. For TLS 1.2 communication, the

server generates a 2048-bit RSA asymmetric key for server authentication and to verify the user authentication information from the AutoPassword Enterprise v4 Android, AutoPassword Enterprise v4 iOS App. It also generates a 256-bit ECDHE asymmetric key used for session key establishment. Additionally, the HASH_DRBG (SHA512) algorithm is used to generate the DEK (Data Encryption Key) used for data encryption and the server, user authentication information used for server, user authentication information generation.

Cryptographic key distribution is as follows. During TLS 1.2 communication, the session key is securely distributed using the ECDHE method. The encryption key for data sent between the AutoPassword Enterprise v4 Server and the business server, and the key for data sent between TOE components, are distributed using RSA 2048 asymmetric encryption.

Cryptographic key derivation is as follows. A 128-bit AES key, used as a Key Encrypting Key (KEK), is derived using PBKDF2 (SHA512) with the user-input password and a 128-bit Salt value as inputs. A 256-bit AES session key is derived using a Key Derivation Function (KDF) with the client random, server random, and shared secret as parameters.

Cryptographic operations are performed using the following cryptographic algorithms.

Standard	Algorithm	Key Length	Operation List
ISO/IEC 29167-10:2017	ARIA-128(CBC)	128	Encryption/decryption of the stored data encryption key using a KEK
			Encryption/decryption of phone numbers and email addresses
			Encryption/decryption for delivering authentication elements and the server/user authentication information generation key to AutoPassword Enterprise v4 Android App, AutoPassword Enterprise v4 iOS App
			Encryption/decryption when storing the server/user authentication information generation key
			Encryption/decryption of the private key password
			Encryption/decryption of DBMS connection

			information
			Encryption/decryption of the SMTP password
ISO/IEC 9797-2	HMAC-SHA256	256	Mutual verification during communicated between TOE components
			Generation of server and user authentication information
RFC 3447	RSA 2048	2048	Digital signature generation and verification for the AutoPassword Enterprise v4 Android App, AutoPassword Enterprise v4 iOS App
			The secret key provided to the business server
			Server verification in TLS 1.2
RFC 5289	AES-256(GCM)	256	TLS 1.2 communication encryption
ISO/IEC 10118-3:2004	SHA256	N/A	Hashing passwords
			TOE Integirty verification
	SHA384	N/A	Integrity check for data communicated between TOE components

[Table 7] Cryptographic Operations List

To generate random bits for cryptographic key generation and other purposes, the TSF performs a deterministic random bit generation service using HASH_DRBG (SHA512) in accordance with NIST SP 800-90A Rev.1 after initialization with a seed. A TSF interface is used for this initialization and seeding.

The TSF updates the DRBG state by reseeding in accordance with NIST SP 800-90A Rev. 1 using the TSF interface getrandom(). This occurs under the following conditions: after 256 generations, when 1 hour has passed since the last seeding, or upon an error.

Furthermore, the TSF seeds the DRBG using the software-based TSF entropy source getrandom(), which provides at least 256 bits of min-entropy. To generate the entropy input for the derivation function defined in NIST SP 800-90A Rev. 1, it performs a Hashing operation on the inputs from TSF interfaces to ensure the final result also has at least 256 bits of min-entropy.

Cryptographic keys are securely destroyed immediately when their purpose is fulfilled or they are no longer needed. All cryptographic keys are made irrecoverable by overwriting their memory region with zeros either one or three times.

▣ Identification and authentication (FIA)

The AutoPassword Enterprise v4 Server provides secure identification and authentication functions to verify the identity of authorized users and administrators, and to restrict their access and use of security functions.

When a user attempts to authenticate, the entered password is visually protected (e.g., displayed as ● characters). If authentication fails, only the failure result is provided, ensuring that specific causes are not exposed externally.

For administrator authentication attempts, an account protection function is activated by detecting the number of consecutive failures. If authentication fails 5 consecutive times, authentication is blocked for 5 minutes, after which it is automatically released.

The administrator's password must meet the following complexity criteria, which include requirements for length, character combination, repetition limits, sequential character prohibition, and reuse prohibition:

- Length must be between 10 and 20 characters, inclusive.
- Must include at least one character from each of the following groups: English uppercase and lowercase letters, numbers, and special characters (@, $, !, %, *, #, ?, &).
- Prohibition of using 3 or more identical consecutive characters or numbers.
- Prohibition of using 4 or more sequential characters or numbers from a keyboard layout.
- Prohibition of using 4 or more sequential numbers.
- Prohibition of using 4 or more sequential alphabetic characters.

TOE generates and verifies the server authentication information used for server authentication and the user authentication information used for user authentication. The server and user authentication information is securely generated and used via HMAC-SHA-256, AES-128-CBC, RSA2048, and SHA-256 cryptographic algorithms. The components required to generate server authentication information include the session ID of the client accessing the business server, generation time, the server and user authentication information generation key, IP address, and digital signature verification

data. The components required to generate user authentication information include the IP address of the AutoPassword Enterprise v4 Android App, AutoPassword Enterprise v4 iOS App, the session ID of the client accessing the business server, the current time, the server and user authentication information generation key, and digital signature verification data.

During the authentication process, a unique random value(nonce) is generated for each session to prevent the reuse of authentication data. This applies to administrator, server, and user authentication.

▣ Security Management (FMT)

The AutoPassword Enterprise v4 Server provides a variety of management functions to securely operate its security features and related data. These functions are designed to be performed only by an authorized administrator.

The administrator can perform account management tasks such as registering, deleting, and modifying user and administrator accounts. They can also manage functions like setting up authenticators for each user, registering, deleting, and modifying integrated services, and issuing and renewing related keys.

Session-related security functions, such as resetting the user authentication failure count and releasing locked sessions, are also controlled through administrator privileges.

Audit records and authentication logs can only be viewed by the administrator, allowing them to track the system's operational status and security incidents.

The administrator can configure the IP addresses allowed to access the web management console and set up the SMTP server and alarm recipient email addresses.

At the administrator's request, an integrity check of the TOE's settings and executable code can be performed.

A function is provided to set the administrator ID and initial password during installation.

The server securely manages various internal security-related data, including identification information, authentication information, log data, and alarm settings for administrators, users, and integrated services. Access to and modification of this data is permitted only for the administrator. and only one administrator account exists.

▣ Protection of the TSF (FPT)

The AutoPassword Enterprise v4 Server provides various Protection of the TSF mechanisms to ensure the reliability of its security functions and to maintain the system's own integrity and stability.

It preserves a secure state even if a failure occurs during the generation of server and user authentication information. The process is safely terminated to prevent the error from affecting the entire system.

When TSF data is transmitted between TOE components, it is protected from unauthorized disclosure or modification. TSF data is always transmitted through a secure path.

Sensitive TSF data such as the asymmetric key for server authentication in TLS 1.2, the asymmetric key for verifying user authentication information from the App, the stored data encryption key, the encryption key for data transmitted between the Server and the business server, the encryption key for data transmitted between TOE components, the server and user authentication information generation key, TOE settings stored in the DBMS, the private key password, the SMTP password, DBMS connection information, the administrator password, and audit data is protected from unauthorized disclosure and modification when stored.

The server automatically performs self-tests and integrity verification during start-up and continues to perform them periodically during normal operation. The administrator can also initiate an integrity check of the server upon request.

The AutoPassword Enterprise v4 Android App, AutoPassword Enterprise v4 iOS App automatically performs self-tests and integrity verification during start-up.

▣ TOE access (FTA)

The AutoPassword Enterprise v4 Server limits the number of administrator sessions and their connection conditions to prevent the misuse of system resources and ensure secure access to the management interface.

Only a single session is permitted for the same administrator account; multiple

concurrent sessions cannot be maintained. This prevents security threats such as session hijacking and duplicate logins.

After an administrator logs in, the session is automatically terminated if there is no activity for 10 minutes. This minimizes the security risks caused by unnecessarily open sessions.

Session establishment is controlled based on the connecting IP address. Attempts to access the management console from an unregistered IP address are blocked. This proactively prevents access from untrusted locations.

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identification	Date
AutoPassword Enterprise v4 Installation Manual v1.1 (AutoPassword Enterprise v4 Installation Manual v1.1.pdf)	November 06, 2025
AutoPassword Enterprise v4 User Manual v1.1 (AutoPassword Enterprise v4 User Manual v1.1.pdf)	November 06, 2025

[Table 8] Documentation

7. TOE Testing

The evaluator conducted independent testing listed in Independent Testing Report [4], based upon test cases devised by the evaluator. The evaluator took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no.: Identifier of each test caser
- Test Purpose: Includes the security functions to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator set up the test configuration and testing environment consistent with the ST [3]. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover weakness analysis of privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing. The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the Penetration Testing Report [5].

8. Evaluated Configuration

The TOE is software consisting of the following components:
TOE: AutoPassword Enterprise v4 (v4.0.3)

- AutoPassword Enterprise v4 Server v4.0.1
- AutoPassword Enterprise v4 Android App v4.0.1
- AutoPassword Enterprise v4 iOS App v4.0.1

The Administrator can identify the complete TOE reference after installation using the product's Info check menu. And the guidance documents listed in this report chapter 7 were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility wrote the evaluation result in the ETR which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC [1] and CEM [2]. The TOE was evaluated based on Common Criteria for Information Technology Security Evaluation. (EAL1).

1. Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE

description), and these three descriptions are consistent with each other. Therefore, the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore, the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defined the security problems that the TOE and operational environment are intended to address. Therefore, the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives for the operational environment are clearly defined. Therefore, the verdict PASS is assigned to ASE_OBJ.1.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore, the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and they are internally consistent. Therefore, the verdict PASS is assigned to ASE_REQ.1.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore, the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict **PASS** is assigned to the assurance class ASE.

2. Development Evaluation (ADV)

The functional specifications specify a high-level description of the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. Therefore, the verdict PASS is assigned to ADV_FSP.1.

The verdict **PASS** is assigned to the assurance class ADV.

3. Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore, the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore, the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict **PASS** is assigned to the assurance class AGD.

4. Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.

The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore, the verdict PASS is assigned to ALC_CMS.1.

Also, the evaluator confirmed that the correct version of the software is installed in device.

The verdict **PASS** is assigned to the assurance class ALC.

5. Test Evaluation (ATE)

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation.

Therefore, the verdict PASS is assigned to ATE_IND.1. Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict **PASS** is assigned to the assurance class ATE.

6. Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don't allow attackers possessing basic attack potential to violate the SFRs.

The verdict **PASS** is assigned to the assurance class AVA.

7. Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	
ATE	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	PASS
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 9] Evaluation Result Summary

10. **Recommendations**

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The TOE must be installed and operated in a physically secure environment accessible only by authorized administrators and should not allow remote management from outside.
- The administrator shall maintain a safe state such as application of the latest security patches, eliminating unnecessary service, change of the default ID/password, etc., of the operating system and DBMS in the TOE operation.
- The administrator should periodically check a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup to prevent audit data loss.
- The developer who uses the TOE to interoperate with the user identification and authentication function in the operational environment of the business system shall ensure that the security functions of the TOE are securely applied in accordance with the requirements of the manual provided with the TOE.

11. Security Target

AutoPassword Enterprise v4 Security Target v1.2[3] is included in this report for reference.

12. Acronyms and Glossary

(1) Acronyms

CC Common Criteria
CEM Common Methodology for Information Technology Security Evaluation
EAL Evaluation Assurance Level
ETR Evaluation Technical Report
SAR Security Assurance Requirement
SFR Security Functional Requirement
ST Security Target
TOE Target of Evaluation
TSF TOE Security Functionality
TSFI TSF Interface

(2) Glossary

Business Server
A server that provides the business services that users want to access.
Authorized Administrator
Authorized user to securely operate and manage the TOE

Authorized User
The TOE user who may, in accordance with the SFRs, perform an operation

Data Encryption Key (DEK)
Key that encrypts and decrypts the data

Decryption
The act that restoring the ciphertext into the plaintext using the decryption key

Encryption

The act that converts the plaintext into the ciphertext using the encryption key

External Entity

Human or IT entity possibly interacting with the TOE from outside of the TOE bounadary

Key Encryption Key (KEK)

Key that encrypts and decrypts another cryptographic key

Private Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is uniquely associated with an entity (the subject using the private key), not to be disclosed

Public Key

A cryptographic key which is used in an asymmetric cryptographic algorithm and is associated with an unique entity (the subject using the public key), it can be disclosed

Public Key (asymmetric) cryptographic algorithm

A cryptographic algorithm that uses a pair of public and private keys

Random bit generator

A device or algorithm that outputs a binary string that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the string can be combined into a random bit block. The RBG is classified into the deterministic

and non-deterministic type. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a “seed key,” and the non-deterministic type RBG produces output that depends on the unpredictable physical source.

Secret Key

Cryptographic key that is used along with a secret key cryptographic algorithm and can be uniquely combined with an entity or more / It shall not be made public.

Self-test

Pre-operational or conditional test executed by the cryptographic module

Symmetric cryptographic technique

Encryption scheme that uses the same secret key in mode of encryption and decryption, also known as secret key cryptographic technique

TSF Data

Data for the operation of the TOE upon which the enforcement of the SFR relies

13. **Bibliography**

The evaluation facility has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-001 ~ CCMB-2022-11-005, November, 2022

[2] Common Methodology for Information Technology Security Evaluation, CC:2022 Revision 1, CCMB-2022-11-006, November, 2022

[3] AutoPassword Enterprise v4 Security Target v1.2, November 6, 2025

[4] AutoPassword Enterprise v4 Independent Testing Report(ATE_IND.1) V1.00, November 27, 2025

[5] AutoPassword Enterprise v4 Penetration Testing Report(AVA_VAN.1) V1.00, November 27, 2025

[6] AutoPassword Enterprise v4 Evaluation Technical Report V1.00, November 27, 2005