National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
for
Thycotic Secret Server Government Edition v10.1

Report Number: **CCEVS-VR-VID10953**
Dated: **December 21, 2018**
Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Daniel P. Faigin

Marybeth S Panock

Jerome F. Myers

The Aerospace Corporation

Evaluation Team

Fathi Nasraoui

CygnaCom Solutions

Table of Contents

List of Figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product Thycotic Secret Server Government Edition v10.1 as defined in the Thycotic Secret Server Security Target, version 2.4.

The Target of Evaluation (TOE) is an Enterprise Security Management application as defined by the Protection Profile for Enterprise Security Management - Identity and Credential Management Version 2.1: "*This protection profile focuses on the aspect of ESM that is responsible for enforcing identity and credential management. Identity and Credential Management products will generate and issue credentials for subjects that reside within the enterprise. They will also maintain the organizational attributes that are associated with these subjects".*

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in December 2018. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is:

- Common Criteria Version 3.1 Revision 4 [CC] Part 2 extended and Part 3 conformant
- Demonstrates exact compliance to Protection Profile for Enterprise Security Management - Identity and Credential Management Version 2.1 as changed/clarified by all applicable Technical Decisions

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org.

2. Identification

Target of Evaluation:	Thycotic Secret Server Government Edition v10.1
Evaluated Configuration:	Thycotic Secret Server Government Edition v10.1, build 104.000003 installed on a platform running: • Microsoft Windows Server 2016 Standard (x64) • Microsoft .NET Framework 4.6.2 • Microsoft's Internet Information Services (IIS) 10.0 • Microsoft SQL Server 2016 With support from the Operating Environment for: • Syslog Server • Active Directory (AD) Server • CRL Server
ST Title:	Thycotic Secret Server Security Target Version 2.4
Developer:	Thycotic
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5200 McLean, VA 22102
Evaluators:	Fathi Nasraoui
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Daniel P. Faigin, Marybeth S Panock, Jerome F. Myers,
CC Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4
PP Identification:	Protection Profile for Enterprise Security Management - Identity and Credential Management Version 2.1

3. Security Policy

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

- SF. Enterprise Security Management
- SF. Security Audit
- SF. Cryptographic Support
- SF. Identification and Authentication
- SF. Security Management
- SF. Protection of the TOE Security Function (TSF)
- SF. TOE Access
- SF. Trusted Path/Channels

3.1. Enterprise Security Management

TOE users authenticate either locally using direct login, or remotely via a configured domain controller in the operational environment. The TOE requires each user to present a valid username and password to gain access to the TOE.

The TOE securely integrates with Active Directory (AD) using LDAP servers. The TOE synchronizes with AD and can use both individual and group membership to grant access to specific IT resources. Additionally, the TOE is capable of creating and managing local user credentials independently from the domain controller.

3.2. Security Audit

The TOE is able to generate audit records for security-relevant events as they occur. Audit data includes date, time, event type, subject identity, and other data as required. The TOE uses the Windows Event Log for storing local audit trail, and is capable of uploading logs to an external audit server over a secure channel.

3.3. Cryptographic Support

The TOE relies on the host platform's operating system for protocol and cryptographic functionality. Windows Server 2016 Standard (x64) implements a certified Cryptographic Primitives Library that is utilized for all cryptographic operations.

The following NIST approved cryptographic algorithms were evaluated by the CAVP and used by the Cryptographic Primitives Library:

Cryptographic Operation	Implementation	Certificate
Cryptographic Signature Generation and Verification	RSA signature generation and verification modulo 2048-bits or greater conforming to FIPS PUB 186-4 “Digital Signature Standard (DSS)”, Section 5.5 using PKCS v1.5 RSA signature generation and verification implemented by the cryptographic library operating in the FIPS mode.	RSA:#2193
Cryptographic Key Generation	RSA key generation using key sizes of 2048-bit or greater that meet FIPS PUB 186-4 “Digital Signature Standard (DSS)”, Appendix B.3	RSA:#2195
Encryption and Decryption	AES operating in CBC, GCM and counter modes for data encryption/decryption implemented to meet FIPS PUB 197, “Advanced Encryption Standard (AES)” in compliance with NIST SP 800-38A and NIST SP800-38D. Encryption/decryption performed by the cryptographic library operating in the FIPS mode.	AES:#4064
Secure Hashing	SHA-1, SHA-256, SHA-384, and SHA-512 cryptographic hashing implemented to meet FIPS PUB 180-4, “Secure Hash Standard”, is performed by the cryptographic library operating in the FIPS mode.	SHS:#3347
Keyed-hash message authentication	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 keyed-hash message authentication implemented to meet FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code”, and FIPS PUB 180-4, “Secure Hash Standard” is performed by the cryptographic library operating in the FIPS mode.	HMAC:#2651
Random bit generation	CTR_DRBG (AES-256) random bit generation implemented to meet NIST SP 800-90A is performed by the cryptographic library running in the FIPS mode.	DRBG:#1217
Component Validation Test	TLSv1.1, TLSv1.2	CVL #886

3.4. Identification and Authentication

The TOE associates all a user’s security attributes with the subjects acting on the behalf of that user. Users receive their privileges either directly or by way of membership in groups and/or roles.

3.5. Security Management

The TOE restricts management functions to authorized administrators. An administrator will authenticate to the TOE by providing their local or domain user credentials. The TOE maintains the following default roles: Read-only, User, Administrator. Each

authenticated user is automatically associated by TSF with a role that determines the user's authorization(s).

3.6. Protection of the TOE Security Functions (TSF)

The TOE protects authentication data, such as stored passwords, so they are not accessible in plaintext. The TOE's certificates and private keys are protected by the Windows Server 2016 Access Control List (ACL) and Data Protection API (DPAPI). The Operational Environment implements and manages both the Certificate Store and the DPAPI, that are accessed using the Microsoft CryptoAPI.

3.7. TOE Access

The TOE is capable of displaying a login banner to all users. The TOE also enforces inactivity timeouts.

3.8. Trusted Path/Channels

The TOE, in the evaluated configuration, exports audit records to an external audit server and synchronizes with an external authentication server over a secure channel. The TOE utilizes IIS web server to implement secure remote administration. IIS implements the TLS v1.1 or TLS v1.2 protocol and supports X.509v3 certificate-based server authentication.

4. Assumptions and Clarifications of Scope

4.1. Usage and Environmental Assumptions

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services;
- There will be a defined enrollment process that confirms user identity before the assignment of credentials;
- The TOE will be able to establish connectivity to other ESM products to share security data;
- Third-party entities that exchange attribute data with the TOE are assumed to be trusted;
- There will be one or more competent individuals assigned to install, configure, and operate the TOE; and
- The TOE will receive reliable time data from the Operational Environment.

4.2. Clarification of Scope

The TOE utilizes the host platform's cryptographic module that implements CAVP validated cryptography.

The TOE supports many features that are not part of the core functionality. Those features are excluded from scope of the evaluation:

- Use of SMTP
- Use of SAML
- Integration with an HSM
- Use of automatic account discovery
- Use of remote password changing functionality, except for Windows Account, Active Directory Account, and Unix Account (SSH)
- Use of session launcher, except for Putty Launcher and RDP Launcher
- Use of automatic patching
- Use of desktop or smartphone apps, only Web UI access was evaluated
- Use of a remote database server, the database was installed locally during the evaluation
- High availability deployments and backup functionality
- Use of SQL Server Express

- Use of IPv6 (only IPv4 was covered by testing)

5. Architectural Information

The TOE is a software application that runs on Microsoft Windows Server 2016 Standard Edition server with IIS enabled and Microsoft SQL Server 2012 database installed locally.

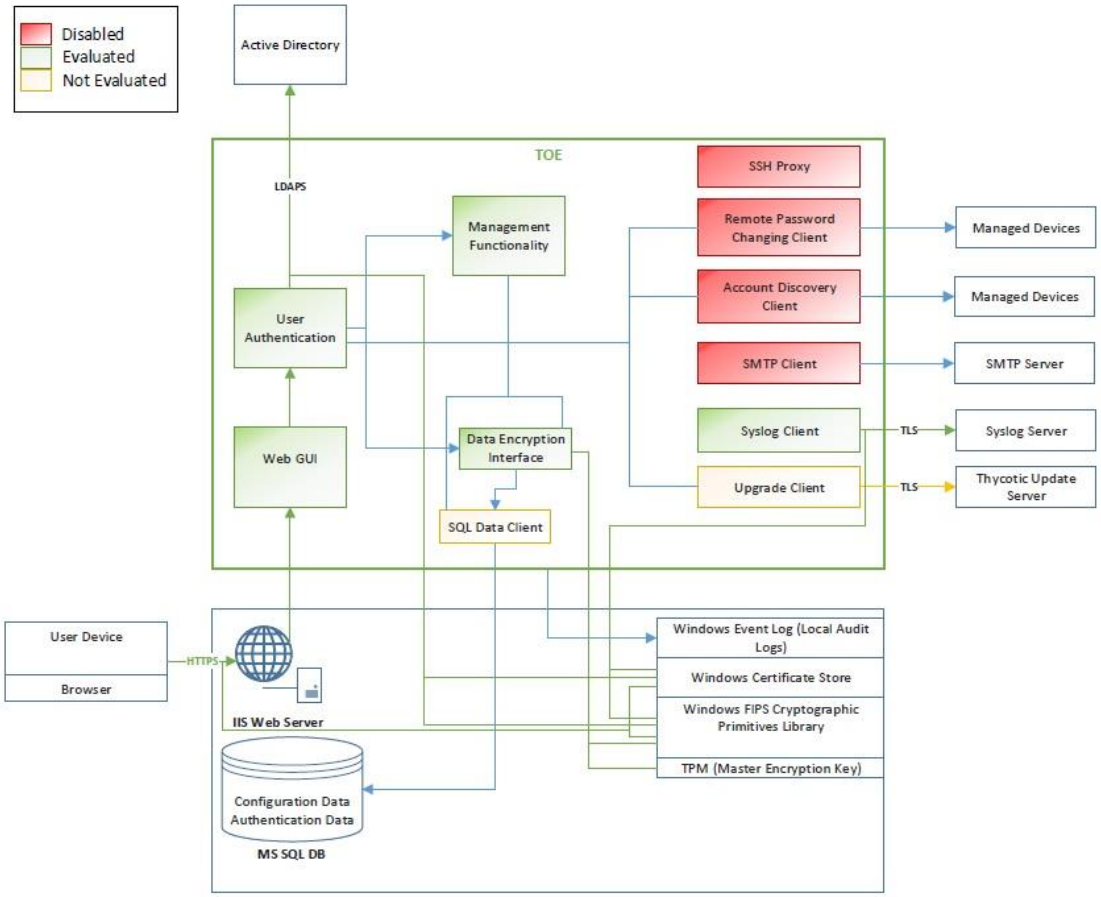

Figure 1: TOE Boundary

The TOE is a software application that is installed on the operating system running on the server hardware. The TOE does not include the hardware or the operating system upon which it is installed. The TOE is delivered as an MSI installer package compatible with Windows Installer 5.0 that deploys ASP.NET application. The package is downloaded from the vendor's secure website.

The TOE relies on the following platform services that are provided by the host system:

- Operating System
    - Cryptographic Primitives Library
- SQL Database
- Web Server (IIS)

The TOE relies upon the Operational Environment for the following Security functionality:

- External Audit Storage
- Domain Controller
- Certificates Authority and Revocation Checking

6. Documentation

The following documents were available for the evaluation. These documents are developed and maintained by Thycotic and delivered to the end user of the TOE:

6.1. User Documentation

1. Thycotic Common Criteria Hardening Guide, Secret Server v10.1, Document Version 1.003, December 17, 2018
2. Thycotic Secret Server User Guide Secret, Secret Server Government Edition v10.0, Document Version 1.1 July 2018
3. Thycotic Secret Server Getting Started Guide, Secret Server Government Edition v10.0 Document version 1.1, July 2018

7. Evaluation Activities

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Evaluation Technical Report for Thycotic Secret Server Government Edition v10.1* document. The evaluation analysis activities involved a structured evaluation of the TOE.

7.1. Guidance Documents

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

7.2. Life-Cycle Support

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.

7.3. Vulnerability Analysis

The evaluators analyzed the list of third party components and determined it to be complete and reasonable. The evaluators then performed a vulnerability search on each component and determined there are no unmitigated vulnerabilities that are introduced by unpatched components. The evaluators then performed a vulnerability search for the product itself and determined there are no outstanding vulnerabilities.

7.4. Development

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements (SFRs). The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

7.5. Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

The test setup was physically located in the dedicated lab environment, with all OE Servers and the TOE connected to an isolated test network that was dedicated to this project. The setup consisted of a 192.168.0.x/16 IPv4 network with all servers assigned static IPv4 addresses within that class. The TOE's IPv6 capability was not tested during the evaluation. The TOE was installed on a dedicated blade server, other OE servers were installed in Virtual Machines (VMs). All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The independent functional tests yielded the expected results and met all the assurance activities, providing assurance that the TOE behaves as specified in the ST and functional specification.

8. Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4.

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 version 3.1 R4 of the CC and the CEM. Additionally, the evaluators performed the assurance activities specified in the Protection Profile for Enterprise Security Management - Identity and Credential Management Version 2.1

The evaluation determined the TOE meets the SARs contained the PP.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR) and the Test Report (TR) which are controlled by CygnaCom CCTL (proprietary).

All assurance activities and work units received a passing verdict. The following components are taken from CC part 3:

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.1 Labelling of the TOE
- ALC_CMS.1 TOE CM coverage
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.1 Security objectives
- ASE_REQ.1 Derived security requirements
- ASE_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability survey

The evaluators concluded that the overall evaluation result for the target of evaluation is PASS. The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

9. Validators Comments/Recommendations

1. There are several recommendations made by the CCTL in the evaluation documents that are worthy of inclusion and highlight to potential users:
    a. The CCTL recommends that network administrators configure x.509v3 certificate-based authentication and enable Secure LDAP when configuring Active Directory
    b. Use of the SQL Server Express is not intended for production environments, and was not covered by evaluation testing.
2. The end-user should be aware that the vendor's numbering scheme for the government edition is different from that used for the generic (commercial) editions, with Government Edition 10.1 being based on Commercial version 10.5. This is significant for those researching CVEs, as CVEs for the non-government versions of this product prior to 10.5 do not apply to validated version of the product.
3. Section 10.2 of the hardening guide includes a list of Secret Templates that are compliant with Common Criteria standards available in the Government edition of Secret Server. Of these, only Windows Account, Active Directory Account, and Unix Account (SSH) Secrets are transmitted to other products. While supported by the product, the other forms of templates do not correspond to ESM SFRs and were not covered by testing. However, they are stored and protected using the same mechanism as the evaluated Secrets.
4. The test set-up used an IPv4 network. The TOE's IPv6 capability was not tested during the evaluation.
5. This product extends Active Directory (itself a form of ESM) to provide Secret management and authenticator / password management for access to the specifically identified types of compatible ESM systems. This is a useful function, but it is important to recognize that it does depend on Active Directory/LDAP for the underlying definition of Enterprise Users.

10. Glossary

10.1. Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

CC	Common Criteria [for IT Security Evaluation]
FIPS	Federal Information Processing Standards Publication
HTTPS	HyperText Transmission Protocol, Secure
IT	Information Technology
NIST	National Institute of Standards and Technology
PP	Protection Profile
RDP	Remote Desktop Protocol
SAR	Security Assurance Requirements
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UI	User Interface

10.2. Terminology

This section defines the product-specific and CC-specific terms. Not all of these terms are used in this document.

Assignment	The specification of an identified parameter in a component.
Assurance	Grounds for confidence that an entity meets its security objectives.
Authorized user	A user who may, in accordance with the SFR, perform an operation.
Class	A grouping of families that share a common focus.
Component	The smallest selectable set of elements on which requirements may be based.

Dependency	A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package..
Element	An indivisible security requirement.
Evaluation	Assessment of a PP, an ST, or a TOE against defined criteria.
Evaluation authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted community.
Evaluation scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
Family	A grouping of components that share security objectives but may differ in emphasis or rigor.
Iteration	The use of the same component to express two or more distinct requirements.
Object	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
Organizational security policies	A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.
Package	A named set of either functional or assurance requirements (e.g. EAL 3).
Protection Profile (PP)	An implementation-independent statement of security needs for a TOE type.
Refinement	The addition of details to a component.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Secret	Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.

Secure state	A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.
Security attribute	A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.
Security Function Policy (SFP)	A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions.
Security Target (ST)	An implementation-dependent statement of security needs for a specific identified TOE.
Selection	The specification of one or more items from a list in a component.
Subject	An active entity in the TOE that performs operations on objects.
Target of Evaluation (TOE)	A set of software, firmware and/or hardware possibly accompanied by guidance.
TOE resource	Anything useable or consumable in the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.
Trusted path	a means by which a user and a TSF can communicate with necessary confidence.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
TSF interface (TSFI)	A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.

11. 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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Thycotic Secret Server Security Target, Version 2.4, December 17, 2018
6. Thycotic Common Criteria Hardening Guide, Secret Server v10.1, Document Version 1.003, December 17, 2018
7. Thycotic Secret Server User Guide Secret, Secret Server Government Edition v 10.0, Document Version 1.1 July 2018
8. Thycotic Secret Server Getting Started Guide, Secret Server Government Edition v 10.0 Document version 1.1, July 2018
9. Evaluation Technical Report for Thycotic Secret Server Government Edition v10.1, Version 1.0, December 19, 2018
10. Test Report Document Version 1.2 December 18, 2018 VID #: 10953 Thycotic Secret Server Government Edition by Thycotic