Thycotic Secret Server
Security Target

Version 1.5
October 22, 2018

Prepared For:

1191 17th Street NW, Suite 1102
Washington DC 20036

Prepared By:

1000 Innovation Drive ♦Kanata, ON K2K 3E7♦Canada

Table of Contents

Figures and Tables

1 Security Target Introduction

This section contains the Security Target (ST) and Target of Evaluation (TOE) identification information and an overview.

1.1 Security Target Reference

ST Title: Thycotic Secret Server Security Target

ST Version: v1.5

ST Author: CygnaCom Solutions Inc.

ST Date: 10/22/2018

1.2 TOE Reference

TOE Developer: Thycotic

Evaluation Sponsor: Thycotic

TOE Identification: Thycotic Secret Server Government Edition v10.0, build 104.000003

Software	Platforms
Thycotic Secret Server Government Edition v10.0	Microsoft Windows Server 2012 R2 (x64) running on Intel Xeon E5 with AES-NI
	Microsoft Windows Server 2012 R2 (x64) running on Intel Core i7 with AES-NI
	Microsoft Windows Server 2012 R2 (x64) running on Intel Core i5 with AES-NI

Table 1: TOE Platforms and Devices

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

Assurance Level: Protection Profile Conformant

1.3 TOE Overview

1.3.1 *TOE Product Type*

The Target of Evaluation (TOE) is a software application used in the enterprise settings to define and maintain user credentials within a large organization. The TOE is responsible for

associating users with different sets of privileges with the access to the operational environment resources and services.

1.3.2 *TOE Usage*

The TOE is an application designed to store, distribute, change, and audit use of enterprise user credentials in a secure environment. In the evaluated configuration consists of the software application running on Windows Server 2012 R2 installed on platforms listed in the Table 1.

The TOE is shipped as an installer that deploys the application, pre-requisite components, and performs initial configuration. To ensure secure use, the TOE must be hardened according to the Common Criteria Hardening Guide prior to being put into production environment.

1.3.3 *TOE Security Functionality*

- Enterprise Security Management
  - Enterprise authentication
  - Identity and credential definition
- Security Audit
  - Audit of security-relevant events
  - Secure logging to a remote audit server
- Cryptographic Support
  - TLS v1.1 and TLS v1.2 implementing secure channel
- Identification and Authentication
  - Authentication failure handling
- Security Management
  - Role-based access control
- Protection of the TOE Security Function (TSF)
  - Protection of stored credentials
  - Protection of secret key parameters
- TOE Access
  - Access banner
  - Session timeouts
- Trusted Path/Channels
  - Secure channel for remote administration
  - Secure channel with authorized IT entities

1.4 TOE Description

The TOE, Thycotic Secret Server Government Edition v10.0 is in an enterprise identity and credential management application. The TOE is used as an enterprise credential manager, where the association of attributes of an individual user with specific credentials can be understood as identity management and the ability to change and revoke credentials as a credential management.

1.4.1 *TOE Platform Requirements*

The TOE is a software application that relies on the hardware and features of an underlying platform to operate.

1.4.1.1 *Platform Hardware Requirements*

The TOE designed to run on the server hardware meeting the following minimum requirements:

	Minimum Hardware Requirements
Hardware	**CPU:** Intel Core i5 **RAM:** 8GB **Data storage:** 60GB

Table 2: Hardware requirements

1.4.1.2 *Test Environment*

The TOE was tested in the following configuration and environment:

	Test Environment
Hardware	Dell PowerEdge R710 running Intel Xeon E5
Software	Microsoft Windows Server 2012 R2 (x64) Microsoft .NET Framework 4.5.2 Microsoft's Internet Information Services (IIS) 8.5 Microsoft SQL Server 2016[1]

---

[1] The TOE claims to support SQL Server 2008 and later, but only SQL Server 2016 was tested

Servers	*Audit Server:* CentOS 7 with OpenSSL 1.0.2k and syslog-ng 3.9.1 *Domain Controller:* Microsoft Windows Server 2012 R2 (x64) running AD with LDAPS enabled *CRL Server:* Ubuntu 16.04 LTS with OpenSSL 1.0.2k and Apache2

Table 3: Test Environment

1.4.2 *TOE Boundary*

1.4.2.1 *Physical Boundary*

The physical boundary of the TOE is 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.

1.4.2.2 *Logical Boundary*

The logical TOE boundary is defined by the security functions performed by the TOE.

1.4.2.3 *TOE Architecture*

The TOE is a software application that runs on Microsoft Windows Server 2012 R2 server with Internet Information Service (IIS) enabled and Microsoft SQL Server database installed.
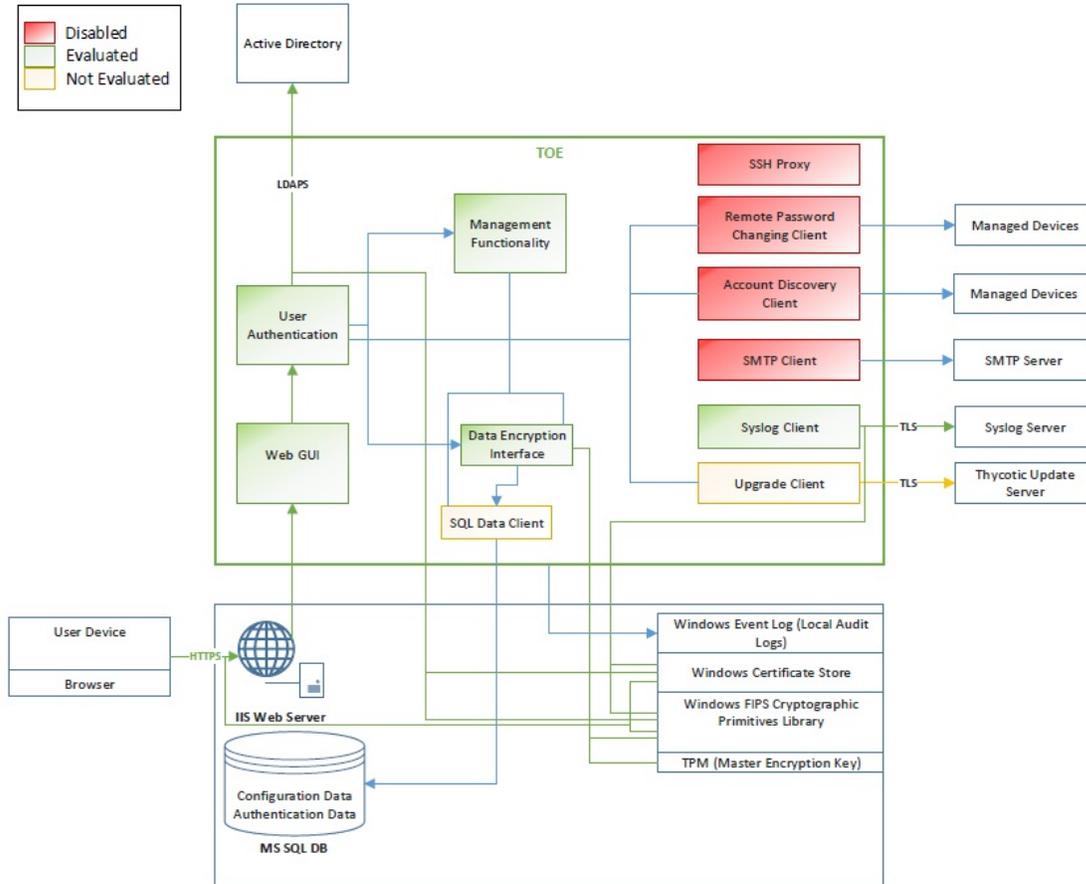
Figure 1: TOE Architecture

1.4.2.4   Management Interface(s)

The TOE supports browser-based management interface secured by HTTPS/TLS. Both local and remote management implemented this way.

1.4.2.5   Operational Environment

The Operational Environment of the TOE includes:
- External management workstation
- Managed devices
- Platform services:
  - Operating System
    - Cryptographic Primitives Library (bcrypt)
  - SQL Database
  - Web Server (IIS)

- External IT services:
  - Syslog Server
  - Active Directory Server
  - CRL Server

1.4.3 *Deployment and Use*

The following figure outlines role of the TOE in the enterprise infrastructure.
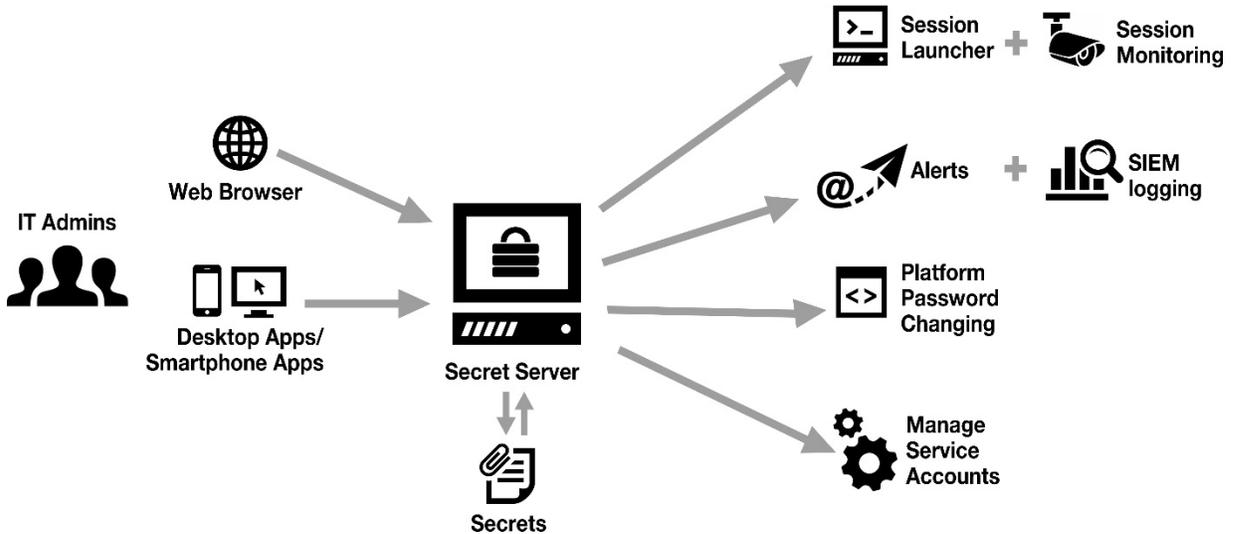
Figure 2: Infrastructure Role

1.4.4 *Excluded Functionality*

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

- Use of the SMTP is not evaluated
- Use of SAML is not evaluated
- Integration with HSM is not evaluated
- Use of automatic account discovery is not evaluated
- Use of remote password changing functionality is not evaluated, except for Unix Account SSH Secrets
- Use of session launcher is not evaluated, except for Putty Launcher used with Unix Account SSH Secrets
- Use of automatic patching is not evaluated

- Use of remote database server is not evaluated, in the evaluated configuration database installed locally
- High availability deployments and backup functionality are not evaluated

1.4.5 *TOE Guidance and Reference Documents*

The following user guidance documents are provided to customers and are considered part of the TOE:

Table 4: TOE Reference Documents

Reference Title	ID
Secret Server User Guide, document version 1.1, July 2018	[ADMIN]
Secret Server Getting Started Guide, document version 1.1, July 2018	
Thycotic Secret Server Functional Specification, document version 0.3, March 14, 2018	[FSP]
Common Criteria Hardening Guide, Secret Server v10.0, document version 1.011, August 2018	[CC Guide]

Documents in the following table were used as reference materials to develop this ST.

Table 5: ST Reference Documents

Reference Title	ID
Common Criteria for Information Technology Security Evaluation, CCMB-2012-09-004, Version 3.1, Revision 4	[CC]
Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, October 24, 2013	[PP]

2 Conformance Claims

2.1 Common Criteria Conformance Claim

This Security Target [ST] and the Target of Evaluation [TOE] are conformant to the following Common Criteria [CC] specifications:

- *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components,* Version 3.1, Revision 4, September 2012, CCMB-2012-09-002
  - o Part 2 Extended

- *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components,* Version 3.1, Revision 4, September 2012, CCMB-2012-09-003
  - o Part 3 Conformant

2.2 Protection Profile Claim

The TOE claims *exact* compliance to *Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1* [ESM ICM PP].

2.3 Package Claim

The TOE does not claim to be conformant with any pre-defined packages.

2.4 Conformance Rationale

This ST claims exact conformance to only one Protection Profile – the ESM ICM PP.

The security problem definition of this ST is consistent with the statement of the security problem definition in the PP, as the ST claims *exact* conformance to the PP and no other threats, organizational security policies, or assumptions are added.

The security objectives of this ST are consistent with the statement of the security objectives in the PP as the ST claims *exact* conformance to the PP and no other security objectives are added.

The security requirements of this ST are consistent with the statement of the security requirements in the PP as the ST claims *exact* conformance to the PP.

2.5 ESM ICM v2.1 Technical Decisions

- TD0320 – TLS ciphers in ESM PPs
  - Removal of mandatory TLS ciphers
  - Applied
- TD0245 – Updates to FTP_ITC and FTP_TRP for ESM PPs
  - Mandatory inclusion of protocol SFRs
  - Applied
- TD0079 – RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
  - Removal of ANS X9.31
  - Not applicable to the evaluation, FCS_RBG_EXT.1 not claimed
- TD0071 – Use of SHA-512 in ESM PPs
  - Added SHA-512 algorithm to FCS_COP.1 selections
  - Not applicable to the evaluation, FCS_COP.1 not claimed
- TD0066 – Clarification of FAU_STG_EXT.1 Requirement in ESM PPs
  - External audit reconciliation is optional
  - Applied
- TD0055 – Move FTA_TAB.1 to Selection-Based Requirement
  - Inclusion of FTA_TAB.1 is conditional
  - Applied
- TD0042 – Removal of Low-level Crypto Failure Audit from PPs
  - Removal of audit events for FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(*), FCS_RBG_EXT.1
  - Not applicable to the evaluation, SFRs not claimed

3 Security Problem Definition

3.1 Threats

This section identifies the threats against the TOE, as specified in the PP, applied verbatim.

Table 6: TOE Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
T.FALSIFY	A malicious user may falsify the TOE's identity and transmit false data that purports to originate from the TOE to provide invalid data to the ESM deployment.
T.FORGE	A malicious user may falsify the identity of an external entity in order to illicitly request to receive security attribute data or to provide invalid data to the TOE.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T. INSUFFATR	An Assignment Manager may be incapable of using the TOE to define identities, credentials, and attributes in sufficient detail to facilitate authorization and access control, causing other ESM products to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
T.RAWCRED	A malicious user may attempt to access stored credential data directly, in order to obtain credentials that may be replayed to impersonate another user.

3.2 Organizational Security Policies (OSPs)

This section identifies the organizational security policies that are expected to be implemented by an organization that deploys the TOE. These OCSP are specified in the PP, copied verbatim.

Table 7: Organizational Security Policies

Policy Name	Policy Definition
P.BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

3.3 Assumptions

This section identifies assumptions applied to the TOE. These assumptions are specified in the PP, copied verbatim. A subset of the optional assumption is included based on the security functionality implemented by the TOE.

Table 8: TOE Assumptions

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

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives for the TOE

This section identifies Security Objectives for the TOE. These objectives have been taken from the PP and copied verbatim. A subset of the optional security objectives is included based on the security functionality implemented by the TOE.

Table 9: TOE Security Objectives

Objective Name	TOE Security Objective Definition
O.ACCESSID	The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.EAVES	The TOE will either leverage a third-party cryptographic suite or contain the ability to use cryptographic algorithms to secure the communication channels to and from itself.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment.
O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
O.INTEGRITY	The TOE will provide the ability to assert the integrity of identity, credential, or authorization data.
O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.PROTCRED	The TOE will be able to protect stored credentials.
O.IDENT	The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.
O.EXPORT	The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels.
O.MANAGE	The TOE will provide Authentication Managers with the capability to manage the TSF.

Objective Name	TOE Security Objective Definition
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.

4.2 Security Objectives for the Operational Environment

This section identifies the security objectives for the operational environment where the TOE is expected to be deployed. These objectives have been taken from the PP. A subset of the optional environment objectives is included based on the security functionality implemented by the TOE.

Table 10: Security Objectives for the Operational Environment

Objective Name	Environmental Security Objective Definition
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.
OE.CRYPTO	The Operational Environment will provide cryptographic mechanisms that are used to ensure the confidentiality and integrity of communications.
OE.ENROLLMENT	The Operational Environment will provide a defined enrollment process that confirms user identity before the assignment of credentials.
OE.FEDERATE	Data the TOE exchanges with trusted external entities is trusted.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.MANAGEMENT	The Operational Environment will provide an Authentication Server component that uses identity and credential data maintained by the TOE.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.

5 Extended Components Definition

The components listed in the following table have been defined in Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1 [ESM ICM PP].

The extended components are denoted by adding "_EXT" in the component name. The extended class is denoted by "ESM_" in the component name.

5.1 Extended Security Functional Components

Table 11: Extended Components

Item	SFR ID	SFR Title
1	ESM_ATD.1	Object Attribute Definition
2	ESM_EAU.2	Reliance on Enterprise Authentication
3	ESM_EID.2	Reliance on Enterprise Identification
5	ESM_ICD.1	Identity and Credential Definition
6	ESM_ICT.1	Identity and Credential Transmission
7	FAU_STG_EXT.1	External Audit Trail Storage
8	FCS_TLS_EXT.1	TLS
9	FPT_APW_EXT.1	Protection of Stored Credentials
10	FPT_SKP_EXT.1	Protection of Secret Key Parameters

5.1.1.1 ESM_ATD.1 Object Attribute Definition

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_ATD.1.1   The TSF shall maintain the following list of security attributes belonging to individual objects: [**assignment: list of object security attributes**].

ESM_ATD.1.2   The TSF shall be able to associate security attributes with individual objects.

5.1.1.2 ESM_EAU.2 Reliance on Enterprise Authentication

Hierarchical to: No other components.

Dependencies: ESM_EID.2 Reliance on Enterprise Identification.

ESM_EAU.2.1   The TSF shall rely on [selection: [**assignment: identified TOE component(s) responsible for subject authentication**], [**assignment: identified Operational Environment component(s) responsible for subject authentication**]] for subject authentication.

ESM_EAU.2.2   The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

5.1.1.3 ESM_EID.2 Reliance on Enterprise Identification

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_EID.2.1   The TSF shall rely on [selection: [**assignment: identified TOE component(s) responsible for subject identification**], [**assignment: identified Operational Environment component(s) responsible for subject identification]**] for subject identification.

ESM_EID.2.2   The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

5.1.1.4 ESM_ICD.1 Identity and Credential Definition

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_ICD.1.1   The TSF shall provide the ability to define identity and credential data for use with other Enterprise Security Management products.

ESM_ICD.1.2   The TSF shall define the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, [**assignment: list of any additional security-relevant identity and credential attributes the TSF is able to associate with enterprise users**].

ESM_ICD.1.3   The TSF shall provide the ability to enroll enterprise users through assignment of unique identifying data.

ESM_ICD.1.4   The TSF shall provide the ability to associate defined security-relevant attributes with enrolled enterprise users.

ESM_ICD.1.5   The TSF shall provide the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6   The TSF shall provide the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7   The TSF shall provide the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

ESM_ICD.1.8   The TSF shall ensure that the defined enterprise user credentials satisfy the following strength rules:

  a) For password-based credentials, the following rules apply:

   1. Passwords shall be able to be composed of a subset of the following character sets: [**assignment: list of character sets that are supported by the TSF for password entry**] that include the following

values [***assignment: list of the supported characters for each supported character set***]; and

2. Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and

3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and

4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based credentials, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2-20.

5.1.1.5 ESM_ICT.1 Identity and Credential Transmission

Hierarchical to:	No other components.
Dependencies:	ESM_ICD.1 Identity and Credential Definition.

ESM_ICT.1 .1   The TSF shall transmit [selection: "identity and credential data", "identity, credential, and object attribute data"] to compatible and authorized Enterprise Security Management products under the following circumstances: [selection: choose one or more of: immediately following creation or modification of data, at a periodic interval, at the request of the product, [***assignment: other circumstances***]].

5.1.1.6 FAU_STG_EXT.1 External Audit Trail Storage

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit Data Generation, FTP_ITC.1 Inter-TSF Trusted Channel.

FAU_STG_EXT.1.1   The TSF shall be able to transmit the generated audit data to [***assignment: non-empty list of external IT entities and/or "TOE-internal storage"***].

FAU_STG_EXT.1.2   The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3   The TSF shall ensure that any TOE-internal storage of generated audit data:

1) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

2) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

5.1.1.7 FCS_TLS_EXT.1 TLS

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation.

FCS_TLS_EXT.1.1   The TSF shall implement one or more of the following protocols [selection: TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites: [selection:

·   TLS_RSA_WITH_AES_128_CBC_SHA
·   TLS_RSA_WITH_AES_256_CBC_SHA
·   TLS_DHE_RSA_WITH_AES_128_CBC_SHA
·   TLS_DHE_RSA_WITH_AES_256_CBC_SHA
·   TLS_RSA_WITH_AES_128_CBC_SHA256
·   TLS_RSA_WITH_AES_256_CBC_SHA256
·   TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
·   TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
·   TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
·   TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
·   TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
·   TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

Note: Modified by TD0320

5.1.1.8 FPT_APW_EXT.1 Protection of Stored Credentials

Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_APW_EXT.1.1   The TSF shall store credentials in non-plaintext form.
FPT_APW_EXT.1.2   The TSF shall prevent the reading of plaintext credentials.

5.1.1.9 FPT_SKP_EXT.1 Protection of Secret Key Parameters

Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_SKP_EXT.1.1   The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.2 Extended Security Functional Components Rationale

All extended security functional components are sourced directly from the PP and applied verbatim.

6 Security Requirements

6.1 Security Functional Requirements

Conventions
The following conventions have been applied in this document:

- **Security Functional Requirements** – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - o **Iteration**: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1 (a) and FDP_ACC.1 (b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, "a" and "b".
  - o **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold italics and are surrounded by brackets (e.g., *[assignment]).*
  - o **Selection**: allows the specification of one or more elements from a list. Selections are indicated using bold text and are surrounded by brackets (e.g., [**selection**]).
  - o **Refinement**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.

Note: Operations already performed in the PP are not identified in this Security Target

- **Explicitly stated Security Functional Requirements** (i.e., those not found in Part 2 of the CC) are identified "_EXT" in the component name.)

- **Case** – ESM ICM PP uses an additional convention which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST.

The TOE security functional requirements are listed in Table 12. All SFRs are based on requirements defined in Part 2 of the Common Criteria or defined in the PP.

Table 12: TOE Security Functional Components

	Functional Component	
1	ESM_ATD.1	Object Attribute Definition
2	ESM_EAU.2	Reliance on Enterprise Authentication
3	ESM_EID.2	Reliance on Enterprise Identification
4	ESM_ICD.1	Identity and Credential Definition
5	ESM_ICT.1	Identity and Credential Transmission
6	FAU_GEN.1	Audit Data Generation
7	FAU_STG_EXT.1	External Audit Trail Storage
8	FCS_TLS_EXT.1	TLS
9	FIA_AFL.1	Authentication Failure Handling
10	FIA_USB.1	User-Subject Binding
11	FMT_MOF.1	Management of Functions Behavior
12	FMT_MTD.1	Management of TSF Data
13	FMT_SMF.1	Specification of Management Functions
14	FMT_SMR.1	Security Management Roles
15	FPT_APW_EXT.1	Protection of Stored Credentials
16	FPT_SKP_EXT.1	Protection of Secret Key Parameters
17	FTA_TAB.1	TOE Access Banner
18	FTA_SSL.3	TSF-initiated Termination
19	FTA_SSL.4	User-initiated Termination
20	FTA_TSE.1	TOE Session Establishment
21	FTP_ITC.1	Inter-TSF Trusted Channel
22	FTP_TRP.1	Trusted Path

6.1.1 *Enterprise Security Management (ESM)*

6.1.1.1 *ESM_ATD.1 Object Attribute Definition*

ESM_ATD.1.1   The TSF shall maintain the following list of security attributes belonging to individual objects: *[as specified in Table 13]*.

Table 13: Object Security Attributes

Object	Attribute
Secret	Secret Template
	Secret Name
	Subject Identifier
	Field Data
	Folder
	Policy Identifier
	Attributes Inherited from Template
	Password Requirements Rule Override
	Command Restrictions
Template	Template Name
	Template Description
	Template Status
	Secret Expiration Policy
	Secret Name Pattern
	Field Parameters (User Name, Password, Type)
	Secret Modification Policy
	Secret Access Policy
	Password Change Policy
	Password Strength Policy

ESM_ATD.1.2   The TSF shall be able to associate security attributes with individual objects.

6.1.1.2 *ESM_EAU.2 Reliance on Enterprise Authentication*

ESM_EAU.2.1   The TSF shall rely on **[*[internal user authentication], [Active Directory]*]** for subject authentication.

ESM_EAU.2.2   The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

6.1.1.3 ESM_EID.2 Reliance on Enterprise Identification

ESM_EID.2.1   The TSF shall rely on **[*[internal user authentication]*, *[Active Directory]*]** for subject identification.

ESM_EID.2.2   The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

6.1.1.4 ESM_ICD.1 Identity and Credential Definition

ESM_ICD.1.1   The TSF shall provide the ability to define identity and credential data for use with other Enterprise Security Management products.

ESM_ICD.1.2   The TSF shall define the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, **[no other attributes]**.

ESM_ICD.1.3   The TSF shall provide the ability to enroll enterprise users through assignment of unique identifying data.

ESM_ICD.1.4   The TSF shall provide the ability to associate defined security-relevant attributes with enrolled enterprise users.

ESM_ICD.1.5   The TSF shall provide the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6   The TSF shall provide the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7   The TSF shall provide the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

ESM_ICD.1.8   The TSF shall ensure that the defined enterprise user credentials satisfy the following strength rules:

    c) For password-based credentials, the following rules apply:

        1. Passwords shall be able to be composed of a subset of the following character sets: **[ASCII, Unicode UTF-8, and Unicode UTF-16 that include the following hexadecimal values 0x0020 to 0x2FA1F];** and

        2. Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and

        3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and

        4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

    d) For non-password-based credentials, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2-20.

6.1.1.5 ESM_ICT.1 Identity and Credential Transmission

ESM_ICT.1 .1   The TSF shall transmit **[identity and credential data]** to compatible and authorized Enterprise Security Management products under the following circumstances: **[immediately following creation or modification of data]**.

6.1.2 Security Audit (FAU)

6.1.2.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1   The TSF shall be able to generate an audit record of the following auditable events:
   a) Start-up and shut-down of the audit functions; and
   b) All auditable events identified in Table 14 for the [not specified] level of audit; and
   c) *[no other auditable events].*

FAU_GEN.1.2   The TSF shall record within each audit record at least the following information:
   a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
   b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *[no other audit relevant information]*.

Table 14: Auditable Events

Component	Auditable Events	Additional Audit Record Contents
ESM_ATD.1	Definition of object attributes	Identification of the attribute defined
	Association of attributes with objects	Identification of the object and the attribute
ESM_EAU.2	All use of the authentication mechanism	No additional information
ESM_EID.2	Creation or modification of identity and credential data	The attribute(s) modified
ESM_ICD.1	Creation and modification of identity and credential data.	The subject created or modified, the attribute(s) modified (if applicable)
	Enrollment or modification of subject	The subject created or modified, the attribute(s) modified (if applicable)

Component	Auditable Events	Additional Audit Record Contents
ESM_ICT.1	Transmission of identity and credential data (and object attributes, if applicable) to external processes or repositories	The destination to which the transmission was attempted
FAU_GEN.1	Start-up and shutdown of the audit functions; All auditable events for the not specified level of audit;	No additional information
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FCS_TLS_EXT.1	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state	Action taken when threshold is reached
FMT_MOF.1	All modifications of TSF function behavior	No additional information
FMT_SMF.1	Use of the management functions	Management function performed
FMT_SMR.1	Modification to the members of the management roles	No additional information.
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	No additional information.
FTA_SSL.4	Termination of an interactive session by the user.	No additional information
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

6.1.2.2 *FAU_STG_EXT.1 Extended: External Audit Trail Storage*

FAU_STG_EXT.1.1   The TSF shall be able to transmit the generated audit data to *[a syslog server, Windows Event Log]*.

FAU_STG_EXT.1.2   The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3   The TSF shall ensure that any TOE-internal storage of generated audit data:

    a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

    b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

6.1.3 *Cryptographic support (FCS)*

6.1.3.1 *FCS_TLS_EXT.1 TLS*

FCS_TLS_EXT.1.1   The TSF shall implement one or more of the following protocols **[TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)]** supporting the following ciphersuites: **[**

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
]

6.1.4 *Identification and Authentication (FIA)*

6.1.4.1 *FIA_AFL.1 Authentication Failure Handling*

FIA_AFL.1.1   The TSF shall detect when **[an administrator configurable positive integer within *[1-99]*]** unsuccessful authentication attempts occur related to *[login attempts]*.

FIA_AFL.1.2   When the defined number of unsuccessful authentication attempts has been **[surpassed]**, the TSF shall *[lock the account]*.

6.1.4.2 *FIA_USB.1 User-Subject Binding*

FAU_USB.1.1   The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: *[user's assigned role that regulate permissions to access objects]*.

FAU_USB.1.2   The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *[associate user's session with user identity]*.

FAU_USB.1.3   The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *[any change is reflected immediately]*.

6.1.5 *Security Management (FMT)*

6.1.5.1 *FMT_MOF.1 Management of Functions Behavior*

FMT_MOF.1.1   The TSF shall restrict the ability to **[determine the behavior of, disable, enable, modify the behavior of]** the functions: *[specified in Table 15]* to *[the specified roles]*.

Table 15: Roles and Management Functions

Role	Management Functions
Read-only	Search and list Secrets
User	Use Secret/Launch session
Administrator	Create, view, expire, edit, and assign Secrets
Administrator	Perform bulk operations on Secrets
Administrator	Create and manage groups
Administrator	Create and manage roles, assign roles to users
Administrator	Create and manage Secret policy
Administrator	Configure TOE SF (see Table 16)
Administrator	Create, manage, and unlock local accounts
Administrator	Configure remote audit server

6.1.5.2 *FMT_MTD.1 Management of TSF Data*

FMT_MTD.1.1   The TSF shall restrict the ability to **[query, modify, delete]** the *[username, password]* to *[administrators]*.

Application Note: All local users have an ability to self-manage their own passwords. Administrator can only reset local user passwords.

6.1.5.3 *FMT_SMF.1 Specification of Management Functions*

FMT_SMF.1.1   The TSF shall be capable of performing the following management functions: *[listed in Table 16]*

Table 16: TOE Management Functions

Requirement	Management Functions
ESM_ATD.1	Definition of object attributes
	Association of attributes with objects
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)
	Management of credential status

Requirement	Management Functions
	Enrollment of users into repository
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed
FAU_STG_EXT.1	Configuration of external audit storage location
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts
	Management of actions to be taken in the event of an authentication failure
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes
FMT_MOF.1	Management of sets of users that can interact with security functions
FMT_SMR.1	Management of the users that belong to a particular role
FTA_SSL.3	Configuration of the inactivity period for session termination
FTA_TAB.1	Maintenance of the banner
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)

6.1.5.4 FMT_SMR.1 Security Management Roles

FMT_SMR.1.1   The TSF shall maintain the roles *[Administrator, User, Read-Only].*

FMT_SMR.1.2   The TSF shall be able to associate users with roles.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_APW_EXT.1 Protection of Stored Credentials

FPT_APW_EXT.1.1   The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2   The TSF shall prevent the reading of plaintext credentials.

6.1.6.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

FPT_SKP_EXT.1.1   The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.1.7 TOE Access (FTA)

6.1.7.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1   *Refinement:* The TSF shall terminate a remote interactive session after an *[Authorized Administrator-configurable time interval of session inactivity]*.

6.1.7.2 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1   *Refinement:* The TSF shall allow *Administrator*-initiated termination of the *Administrato*r's own interactive session.

6.1.7.3 FTA_TAB.1 TOE Access Banners

FTA_TAB.1.1 *Refinement:* Before establishing a user session, the TSF shall display a *configurable* advisory warning message regarding unauthorized use of the TOE.

6.1.7.4 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on *[[IP Address Range]]*.

6.1.8 Trusted Path/Channels (FTP)

6.1.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall be capable of using **[[TLS]]** to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, **[authentication server, no other capabilities]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit **[the TSF]** or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *transfer of policy data**, [transfer of authentication data, transfer of audit data]*.

6.1.8.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall be capable of using **[[TLS]]** to provide a communication path between itself and remote users that is logically distinct from other communication channels and provides assured identifications of its end points and protection of the communicated data from modification, disclosure, and *[[substitution]]*.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication and execution of management functions.

6.2 Security Assurance Requirements

6.2.1 *Security Assurance Requirements for the TOE*

This section defines the assurance requirements for the TOE. The assurance activities to be performed by the evaluator are defined in Section6 of [ESM ICM PP]. The TOE security assurance requirements, summarized in the table below, identify the management and evaluative activities required to address the threats.

Table 17: Assurance Components

Assurance Class	Assurance Components	
Development	ADV_FSP.1	Basic Functional Specification
Guidance documents	AGD_OPE.1	Operational User guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent Testing - Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Survey

The following tables state the developer action elements, content and presentation elements and evaluator action elements for each of the assurance components.

Table 18: ADV_FSP.1 Basic Functional Specification

Developer action elements	
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
Content and presentation elements	
ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
Evaluator action elements	
ADV_ FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_ FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Table 19: AGD_OPE.1 Operational User Guidance

Developer action elements	
AGD_OPE.1.1D	The developer shall provide operational user guidance.
Content and presentation elements	
AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
Evaluator action elements	
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 20: AGD_PRE.1 Preparative Procedures

Developer action elements	
AGD_PRE.1.1D	The developer shall provide the TOE, including its preparative procedures.
Content and presentation elements	
AGD_ PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_ PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
Evaluator action elements	
AGD_ PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_ PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

Table 21: ALC_CMC.1 Labeling of the TOE

Developer action elements	
ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
Content and presentation elements	
ALC_CMC.1.1C	The TOE shall be labeled with its unique reference.
Evaluator action elements	
ALC_CMC.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 22: ALC_CMS.1 TOE CM Coverage

Developer action elements	
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
Content and presentation elements	
ALC_CMS.1.1C	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
Evaluator action elements	
ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 23: ATE_IND.1 Independent Testing – Conformance

Developer action elements	
ATE_IND.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
ATE_IND.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

Table 24: AVA_VAN.1 Vulnerability Survey

Developer action elements	
AVA_VAN.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
AVA_VAN.1.1C	The TOE shall be suitable for testing.

Evaluator action elements	
AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6.2.2 Security Assurance Requirements Rationale

This ST conforms to the [ESM ICM PP], which draws from the CC Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

6.2.3 Extended Assurance Activities

The following subsections define the explicit assurance activities presented in the [ESM ICM PP] for applicable SAR families. These assurance activities serve to refine the standard SARs previously stated with specific activities to be performed by the evaluators during the course of their evaluation.

6.2.3.1 Class ADV Assurance Activities

ADV_FSP.1 Activities

There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described for each SFR, and for other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided. For example, if the TOE provides the capability to configure the key length for the encryption algorithm but fails to specify an interface to perform this function, then the assurance activity associated with FMT_SMF would fail.

The evaluator shall verify that the TOE functional specification describes the set of interfaces the TOE intercepts or works with. The evaluator shall examine the description of these interfaces and verify that they include a satisfactory description of their invocation.

6.2.3.2 Class AGD Assurance Activities

AGD_OPE.1 Activities

Some of the contents of the operational guidance will be verified by the assurance activities with each SFR. The following additional information is also required.

The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the

administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

AGD_PRE.1 Activities

As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms (that is, combination of hardware and operating system) claimed for the TOE in the ST.

6.2.3.3   Class ALC Assurance Activities

ALC_CMC.1 Activities

The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

ALC_CMS.1 Activities

The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

6.2.3.4   Class ATE Assurance Activities

ATE_IND.1 Activities

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluator must document in the test plan that each applicable testing requirement in the ST is covered.

The Test Plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification shall address the differences between the tested platform and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale shall be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used.

The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH).

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

6.2.3.5 Class AVA Assurance Activities

AVA_VAN.1 Activities

As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in this category of ESM application in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.

7 TOE Summary Specification

This chapter describes the security functions:
- Enterprise Security Management (ESM)
- Security Audit (FAU)
- Cryptographic Support (FCS)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of the TSF (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

7.1 Enterprise Security Management (ESM)

ESM_ATD.1

The TOE provides the capability to define objects, called "Secret" in the guidance, that correspond to a broad spectrum of sensitive data. Secret is a data structure, an abstract representation of, and means to securely access a shared managed resource. Individual object attributes are listed in Table 13: Object Security Attributes. The purpose of attributes is to describe the object and to enable control of the object via policies, including attribute based access control.

ESM_EAU.2, ESM_EID.2

The TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. Users authenticate to the TOE by providing a username and password. The TOE users authenticate either locally using direct login, or remotely via a configured domain controller (Active Directory) in the operational environment. When using local login, user credentials are checked against the internal authorized users database. When using domain login, the TOE initiates an authentication request to the external domain controller (Active Directory) using LDAP over TLS, and only allows access after receiving a successful result message.

ESM_ICD.1

The TOE is a gatekeeper of IT resources, and in this capacity also acts as a credential manager server. When acting as a gatekeeper, the TOE enables authenticated users to access a remote computer, network device, database, or a website based on the user's domain or local credentials. The TOE both defines and consumes policy on behalf of ESM products. When the TOE consumes a policy it determines access to a Secret, which is an abstraction of an ESM product, and which is also a means to access the ESM product.

The TOE can manage any IT product compatible with the following types of Secrets or credential types:
- Windows Account

- Active Directory Account
- Cisco Account (SSH)
- HP iLO Account (SSH)
- Unix Account (SSH)
- Web Password
- SQL Server Account

Broadly, these Secrets fall into the following categories: information that can be used to access an IT system, credential data used for authentication to a system.

For password-based credentials, the TOE utilizes a standard character set. All passwords are controlled by an administrator-configurable policy that defines minimum length, composition, aging, and reuse. In the evaluated configuration a minimum password length of 15 characters is required. For non-password based credentials, the TOE utilizes 2048-bit RSA keys that rely on a prime factorization hard problem. The TOE also offers a capability to randomly generate strong passwords.

The TOE integrates with a domain authentication server (Active Directory) and allow users to use their domain credentials to authenticate. Once integrated, the TOE can use domain group membership to control access to individual Secrets or groups of Secrets. The TOE's treats both local and domain accounts in the same way, and local user accounts can be converted to domain accounts via an automated process. The TOE implements configurable behavior on how to handle new domain users. By default, all new domain users have to be explicitly enabled, but the TOE can be configured to automatically associate new domain users with a role based on their domain group membership.

ESM_ICT.1

The TOE implements remote password change functionality that enables administrators to trigger a one-time change or schedule an automatic password rotation of managed platforms. Updated passwords take effect immediately following modification of credential data (Secret) by the TOE. In the evaluated configuration automatic password change functionality is limited to Unix Account (SSH).

The TOE also supports Secure LDAP protocol for communication with a compatible domain authentication server (Active Directory). Synchronization with Active Directory is periodic, with an administrator-configurable polling period.

7.2 Security Audit (FAU)

FAU_GEN.1

The TOE is able to generate audit records of security relevant events as they occur. The events that can result in an audit record are listed in Table 14: Auditable Events. Generally, any use of a management functions via the web interface, as well as relevant IT environment events, will be logged. 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.

Local audit logs are stored as EVT records and include the event level, the date and time of the event, the source of the event, the event ID, and task category. The local audit records can be viewed by authorized OS administrators using Windows Administrative Tools/Event Viewer.

FAU_STG_EXT.1

The TOE stores audit data locally, in the operational environment, by utilizing the Windows Event Log (EVT) system, and remotely by securely uploading audit records to an audit server (syslog) in the operational environment. By default, all event logs are sent to the remote audit server, and the TOE can be configured to duplicate that audit trail to a local Windows Event Log. To implement remote logging the TOE uses the syslog protocol (RFC 5242) encapsulated in the TLS protocol (RFC 5246, RFC 4346) to secure the transmission of the audit data. The TOE relies on Windows Server 2012 R2 Secure Channel (`schannel`) functionality to implement TLS, and as a result of buffering there is a limited log reconciliation functionality. Some of the audit data is stored directly within the TOE boundary in form of various reports; the Operational Environment is expected to protect the internal data, the locally stored EVT audit data, and the audit data during transmission to the external audit server.

7.3 Cryptographic Support (FCS)

FCS_TLS_EXT.1

The TOE supports TLS v1.1 and TLS v1.2 with all claimed ciphers for the use with the external audit and authentication servers.

The following ciphers are supported in the evaluated configuration:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

However cipher settings are OS-wide and not application-specific.

The TLS is implemented by the operational environment, specifically Windows Server 2012 R2 Secure Channel (`schannel`). All protocol operation, including cryptographic primitives, including encryption and decryption, are implemented by the operational environment.

7.4 Identification and Authentication (FIA)

FIA_USB.1

The TOE associates all of 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.

The TOE enforces the following rule on the initial association of user's security attributes with subjects acting on the behalf of users: the user must be successfully authenticated (via the domain controller or locally) for the initial association of attributes to occur.

The user's attributes are tracked against the session maintained by the TOE. Attribute changes for users are immediate and take effect during the user's active session. These attributes are constantly checked with every action a user takes during their session, i.e. accessing folders, secrets, performing administrative functions, etc.

FIA_AFL.1

The TOE is designed to require users to be identified and authenticated before they can access any of the TOE functions. If a user repeatedly fails to authenticate, their account will be locked after an administrator-configurable number of unsuccessful authentication attempts. By default, lockout window is 60 minutes, after which the account is automatically unlocked. Alternatively, an administrator with the correct role permissions must log into Secret Server, navigate to that user in the Administration menu, and manually unlock the user's account.

7.5 Security Management

FMT_MOF.1

The TOE restricts management functions to authorized administrators. An administrator will authenticate to the TOE by providing their local or domain user credentials. If domain credentials are used, the TOE will interface with the remote authentication server. If the local credentials used, local authentication identity store will be checked to determine if the credentials are valid. The TOE will next confirm that the user's account has not been locked or disabled and will then allow the user access to the TSFs that are available to the user's defined role.

FMT_SMF.1

The TOE implements the management functions identified in Table 16: TOE Management Functions. The TSF acting on behalf of authorized users assigned roles listed in the Table 15: Roles and Management Functions performs this functionality.

FMT_SMR.1

The TOE maintains the following default roles: Read-only, User, Administrator. These roles are listed in the Table 15: Roles and Management Functions. Each authenticated user is automatically associated by TSF with a role that determines this user's management authorizations. Authorized administrators also have the ability to create custom roles and assign or remove attributes from the default roles.

FMT_MTD.1

The local authentication data repository is implemented as a table in the Microsoft SQL Server installed in the operational environment. Access to the data stored in this database is secured with a local system account unique to the TOE. The operating system enforces database access permissions and prevents unauthorized access to the authentication data stored there.

The TOE is also capable of integrating with the external Active Directory (AD) domain controller using LDAP over TLS for secure communications.

7.6 Protection of the security functionality

FPT_APW_EXT.1

The TOE protects authentication data, such as stored passwords, so they are not directly accessible in plaintext. Locally stored password information is obscured by use of AES256 encryption. Additionally, when login-related configuration information is accessed through regular TOE interfaces, it is obfuscated by substituting the entered password characters with a series of asterisks.

FPT_SKP_EXT.1

The TOE's client X.509v3 certificates and their associated private keys are protected by the Windows Server 2012 Access Control List (ACL) and Data Protection API (DPAPI). DPAPI is a built-in component of Windows Server 2012 and operates based on symmetric encryption with a randomly-generated Master Key. Trusted CA X509 certificates, or trust anchors, are also managed by the Windows Server 2012 platform and can be accessed using the Windows Certificate Store.

Secrets, when stored in non-volatile memory, are encrypted with the TOE's Master Key, which is in turn is protected by the DPAPI. The Operational Environment implements and manages both the Certificate Store and the DPAPI and accessed using the Microsoft CryptoAPI. The Operational Environment also implements all protocols and manages all public and private keys. The TOE can only access these protocols and keys through a standard API, and does not implement any mechanisms designed to circumvent this functionality.

7.7 TOE access

FTA_TAB.1

The TOE can be configured to display administrator-configured advisory banners as part of the authentication prompt.

FTA_SSL.3

The TOE can be configured by an administrator to force an interactive session timeout value (any positive integer value in minutes). The inactivity timeout is disabled by default and is controlled by the 'Force Inactivity Timeout' setting. A remote session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. Once terminated, the user will be required to re-enter their user name and password so they can establish a new session.

FTA_SSL.4

Any administrative session can be terminated by logging out. Once terminated, the user will be required to re-enter their user name and password or re-authenticate with the domain controller to establish a new session.

FTA_TSE.1 TOE Session Establishment

The TOE can be configured to deny session establishment based on IP Address Range.

7.8 Trusted path/channels

FTP_ITC.1, FTP_TRP.1

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. In order to protect exported audit records and domain authentication data from disclosure or modification, the TOE implements the TLS v1.1 or TLS v1.2 protocol with optional certificate-based (X.509v3) authentication. Trust is established based on Windows Certificate Store. In both of these cases, the TOE acts as a TLS client.

The TOE utilizes Internet Information Services (IIS) web server to offer secure remote administration. The web server implements the TLS v1.1 or TLS v1.2 protocol and supports certificate-based (X.509v3) server authentication. In this case, the TOE acts as a TLS server.

The TOE relies on Windows Server 2012 R2 to provide protocol and cryptographic functionality. Windows Server 2012 R2 is Common Criteria certified (Protection Profile for General Purpose Operating Systems v4.1) and implements a Cryptographic Primitives Library (bcrypt) that is also component validated for TLS key derivation. See Table 25: TOE Certified Cryptography for details. This cryptographic library (bcrypt) is part of the platform and is exclusively utilized to implement cryptographic operations used as part of trusted path/channel functionality.

Table 25: TOE Certified Cryptography

Cryptographic Operation	Implementation	Certificate
Cryptographic Key Generation and Cryptographic Signatures	Implemented by the cryptographic library operating in the FIPS mode. RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater in compliance with FIPS PUB 186-4, "Digital Signature Standard". Cryptographic signature functionality is performed by the cryptographic library operating in the FIPS mode.	RSA:#1487
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:#2832
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:#2373

Cryptographic Operation	Implementation	Certificate
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:#1773
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:#489
Component Validation Test	TLSv1.1, TLSv1.2	CVL #323

Acronyms and Terminology

The following table defines CC and Product specific acronyms used within this Security Target.

Table 26: Acronyms

Acronym	Definition
CC	Common Criteria
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RFC	Request for Comment
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface