Thycotic Secret Server
Security Target

Version 2.4
December 17, 2018

Prepared For:

thycotic

1191 17th Street NW, Suite 1102
Washington DC 20036

Prepared By:

Cygnacom
Solutions

7925 Jones Branch Dr. #5200 ♦ McLean, VA 22102♦ USA

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: v2.4
ST Author: CygnaCom Solutions Inc.
ST Date: 12/17/2018

1.2 TOE Reference

TOE Developer: Thycotic
Evaluation Sponsor: Thycotic
TOE Identification: Thycotic Secret Server Government Edition v10.1, build 104.000003

Software	Platforms
Thycotic Secret Server Government Edition v10.1	Microsoft Windows Server 2016 Standard (x64) running on Intel Xeon E5 with AES-NI
	Microsoft Windows Server 2016 Standard (x64) running on Intel Core i7 with AES-NI
	Microsoft Windows Server 2016 Standard (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 facilitating access of enterprise users with different sets of privileges to the enterprise resources and services.

1.3.2 *TOE Usage*

The TOE is an enterprise application designed to store, distribute, change, and audit use of enterprise user credentials in a secure environment. In the evaluated configuration the TOE consists of the software application running on Windows Server 2016 Standard Edition 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 *Product Overview*

The TOE extends the ability of enrolled Enterprise Users to access systems within the enterprise that are not capable of consuming Enterprise User definitions directly. The TOE accomplishes this through the use of internal objects, called “Secrets”, which are managed by the TOE. To access IT assets, Enterprise Users log into the TOE with their enterprise credentials, and then connect to the managed systems through the TOE, with the TOE providing the credentials on behalf of the Enterprise User.

The TOE, Thycotic Secret Server Government Edition v10.1, integrates with a domain controller and then, based on individual or group identities, offers access to specific IT assets or groups of IT assets, called “Folders”, within the enterprise environment. The TOE is capable of utilizing both existing logins, and generating and automatically rotating strong passwords that it assigns to managed IT assets. These credentials are internally represented by objects called Secrets. The TOE synchronizes with Active Directory (AD) and can use both individual and group membership to grant access. Additionally, the TOE is capable of creating and managing local users independently from AD.

The TOE facilitates access to enterprise products that are not capable of directly integrating with domain controllers. The TOE enables authenticated users to directly access compatible IT assets by using managed credentials with a compatible launcher.

The TOE maintains two types of objects internally: Secrets and Secret Templates. Each Secret inherits all attributes of corresponding Secret Template. Attributes of these objects, among other things, contain the credentials to access a particular enterprise IT asset. These objects contain the credentials required to access a particular enterprise IT asset. When the TOE transmits credentials to managed IT assets, this data takes the form of a user name, password and optionally non-password based credentials such as RSA keys. Secrets are opaque from the point of view of TOE non-administrative users. The purpose of a Secret is to describe and to enable control of a particular IT asset via policies.

The TOE securely integrates with a domain controller (i.e. Active Directory over LDAPS). Once integrated, the TOE can use domain group membership to control access to individual Secrets or groups (Folders) of Secrets.

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

The TOE can manage any IT asset compatible with the following types of credentials:

- Windows Account

- Active Directory Account
- Unix Account (SSH)

These credential types define a broad range of compatible ESM products. Generally, any modern system that supports a specific set of credentials and allows an operator to SSH or RDP into the system is supported. Specifically, Linux 2.6.32 or later, Windows Server 2008 R2 or later, Windows 7 Enterprise or later are compatible. For example, a Unix Account (SSH) Secret would allow managing CentOS 6 based server.

1.3.4 *TOE Security Functionality*

- SF. Enterprise Security Management
    - The TOE extends the identity of enrolled enterprise users to provide audited access to managed IT assets
    - The TOE facilitates remote access to managed IT assets via an integrated launchers
    - The TOE enables authenticated users to directly access compatible IT assets by using managed credentials with a compatible launcher.
- SF. Security Audit
    - The TOE generates audit records of security relevant events as they occur
    - The TOE stores audit records locally and is capable of uploading logs to an external audit server
- SF. Cryptographic Support
    - TLS v1.1 and TLS v1.2
    - The TOE relies on the platform to provide protocol and cryptographic functionality
- SF. Identification and Authentication
    - The TOE associates all users with roles that determine user privileges
    - The TOE requires users to be identified and authenticated to access any of the TOE functionality
    - Repeated failure to authenticate results in account lockouts
- SF. Security Management
    - The TOE restricts management functions to authorized administrators
    - The TOE implements RBAC and maintains Read-only, User, and Administrator roles.
    - The TOE supports local and domain users
- SF. Protection of the TOE Security Function (TSF)
    - The TOE utilizes platform DPAPI to protect sensitive data
    - The TOE relies on Windows Certificate Store to protect certificates
- SF. TOE Access
    - The TOE displays an advisory banner as part of the authentication prompt
    - The TOE enforces session inactivity timeouts

  - The TOE can be configured to restrict access to an IP range
- SF. Trusted Path/Channels
  - The TOE relies on IIS web server to offer secure remote administration
  - The TOE integrates with AD and remote syslog over TLS

As with all evaluations claiming conformance to a standard Protection Profile (PP), the evaluated security functionality is both determined by and tailored to specific component and configuration requirements dictated by exact conformance to the PP. A detailed description of the evaluated security functionality can be found in the Section 7 TOE Summary Specification section of this document.

1.4 TOE Description

The TOE, Thycotic Secret Server Government Edition v10.1, is in an enterprise identity and credential management application. The TOE is used as an enterprise credential manager, where it extends the identity of enrolled enterprise users to provide audited access to enterprise non-person entities or objects that will in turn consume this identity data.

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 Requirements

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

Table 2: Minimum requirements

Minimum Hardware Requirements	
Hardware	**CPU:** Intel 2.4 GHz 4-core 64-bit processor **RAM:** 8 GB **Data storage:** 60 GB of free space **Network:** Gigabit Ethernet adapter
Minimum Software Requirements	
Software	**OS:** Microsoft Windows Server 2016 (x64)[1] **Database:** Microsoft SQL Server 2012[2]

[1] Windows Server 2016 ships with .NET 4.6.2 included; .NET 4.6.2 is backwards compatible with all previous .NET 4.x versions. Microsoft ensures that new .NET framework versions are backwards compatible. The .NET framework is updated through Windows Update, where Microsoft dictates specific release of the .NET framework on a fully patched system.

[2] Use of SQL Server Express, although included in the installation package, was not covered by the evaluation.

1.4.1.2 Test Environment

The TOE was tested in the following configuration and environment:

Table 3: Test Environment

Test Environment	
Hardware	Dell PowerEdge R710 running Intel Xeon E5
Software	Microsoft Windows Server 2016 Standard Edition (x64) Microsoft .NET Framework 4.6.2 Microsoft's Internet Information Services (IIS) 10.0 Microsoft SQL Server 2016
IT Servers	*Audit Server:* CentOS 7 with OpenSSL 1.0.2k and syslog-ng 3.9.1 *Authentication Server:* Microsoft Windows Server 2012 R2 running AD with LDAPS enabled *CRL Server:* Ubuntu 16.04 LTS with OpenSSL 1.0.2k and Apache2

1.4.2 *TOE Boundary*

1.4.2.1 Physical 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 on 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.

1.4.2.2 Logical Boundary

The logical boundary of the TOE is defined by the implemented security functionality (SF) as summarized in Section 1.3.4 TOE Security Functionality and further described in Section 7 TOE Summary Specification of this document. The SF is specified by the Security Functional Requirements (SFRs) listed in Section 6 of this document.

The TOE relies on the host platform, Windows Server 2016 Standard Edition, to partially or fully implement the following SF:

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

The host platform implements the following security services and windows components relevant to the evaluation:

- Microsoft Secure Channle (Schannel), which implements the Transport Layer Security (TLS) for the Trusted Channel with Domain Controller and Audit servers
- Microsoft Internet Information Services (IIS) for the Trusted Path implementing web-based administration
- Windows Certificate Store for certificate-based authentication of Domain Controller, Audit servers, and authentication of TOE's web-based interface
- Access Control List (ACL) to manage the access rights to files and data stored as files
- Data Protection API (DPAPI) functionality to provide operating system-level data protection services to configuration and keys
- Locally installed Microsoft SQL Server 2016 database to store and protect objects and user data.

The remaining SF is implemented as an ASP .NET software application running on .NET 4.6.2 or later framework. Please see Section 1.4.2.3 TOE Architecture Figure 1 for details.

1.4.2.3 TOE Architecture

The TOE is a software application that runs on Microsoft Windows Server 2016 Standard Edition server with Internet Information Service (IIS) enabled and Microsoft SQL Server database installed.

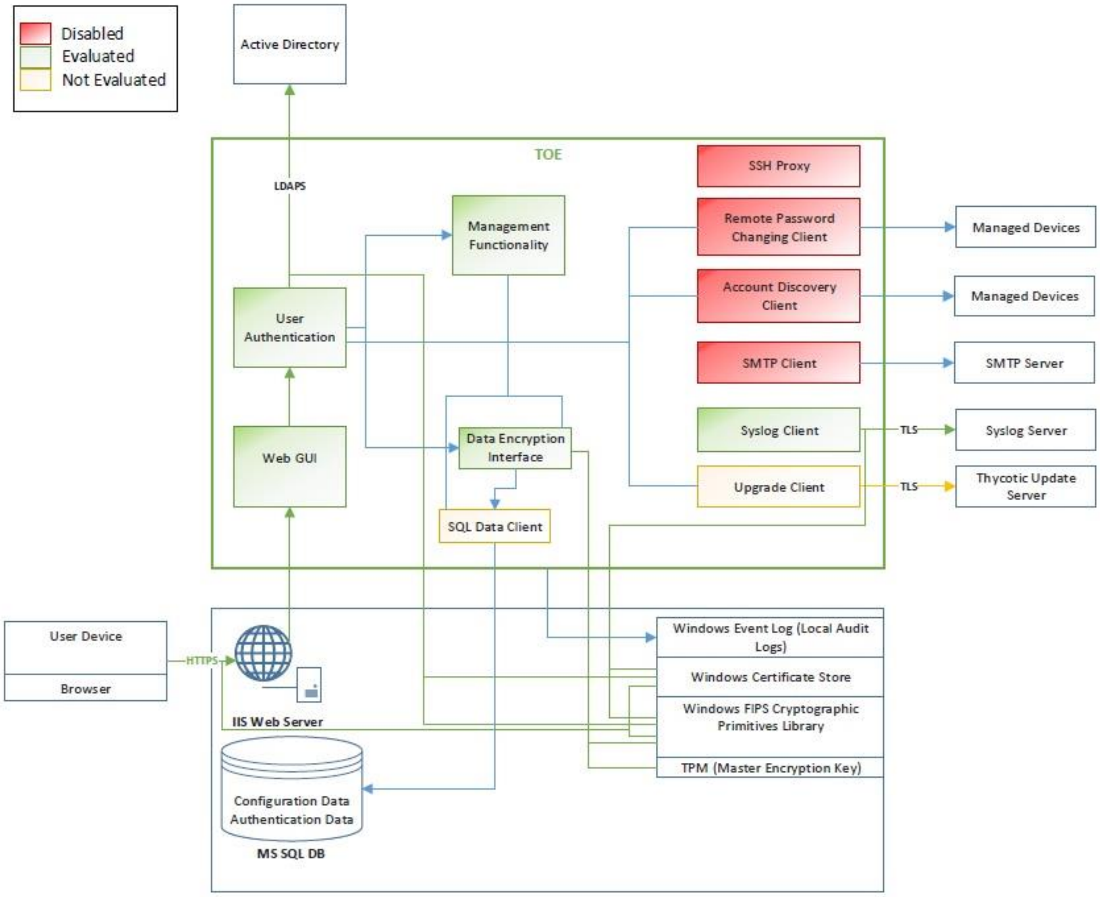

Figure 1: TOE Architecture

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 TOE, Thycotic Secret Server Government Edition v10.1, integrates with a domain controller and then, based on individual or group identities, offers access to specific IT assets or groups of IT assets within the enterprise environment. The TOE is capable of utilizing both existing logins, and generating and automatically rotating credentials that it assigns to IT assets. These managed credentials are internally represented by objects called Secrets. Secrets are opaque from the point of view of TOE non-administrative users.

The TOE synchronizes with Active Directory (AD) and can use both individual and group membership to grant access to Secrets. Additionally, the TOE is capable of creating and managing local users independently from AD.

The TOE is deployed on Windows Server 2016 Standard Edition with locally installed Microsoft SQL Server 2016 database. IT assets are accessed via web-browser initiated session launcher.

The following figure illustrates the role of the TOE in the enterprise infrastructure.

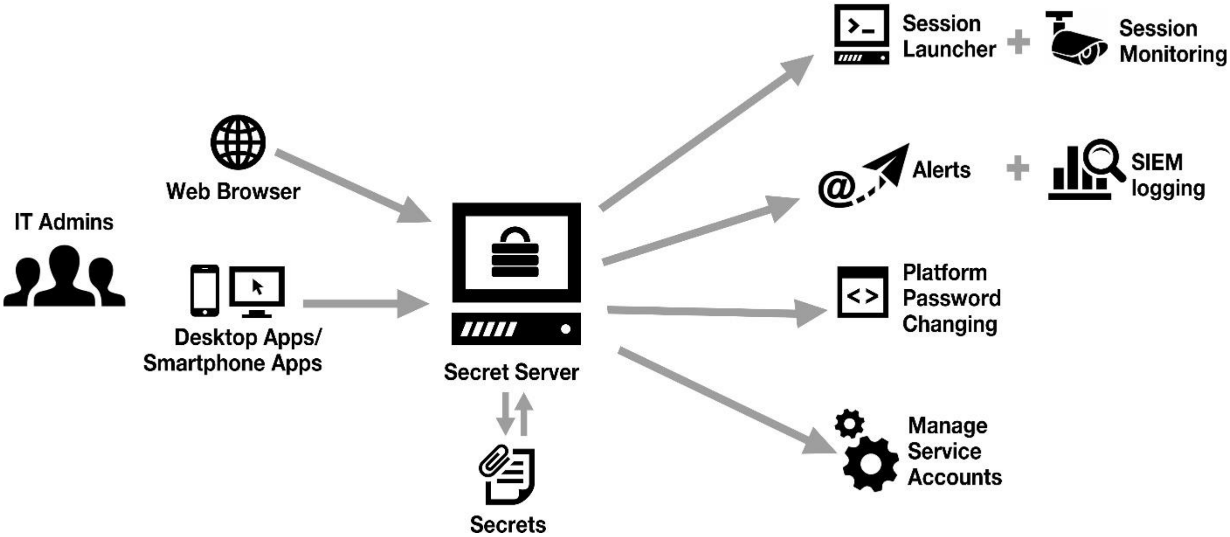

Figure 2: Infrastructure Role

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 was not evaluated

- Use of SAML is not evaluated
- Integration with HSM was not evaluated
- Use of automatic account discovery was not evaluated
- Use of remote password changing functionality is not evaluated, except for Windows Account, Active Directory Account, and Unix Account (SSH)
- Use of session launcher is not evaluated, except for Putty Launcher and RDP Launcher
- Use of automatic patching was not evaluated
- Use of desktop or smartphone apps was not evaluated, only browser-based access was used during evaluation
- Use of remote database server was not evaluated, in the evaluated configuration database was installed locally
- High availability deployments and backup functionality was not evaluated
- Use of SQL Server Express was 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 0.4, September 24, 2018	[FSP]
Common Criteria Hardening Guide, Secret Server v10.1, document version 1.003, December 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*
    - 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*
    - 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_EAU.2	Reliance on Enterprise Authentication
2	ESM_EID.2	Reliance on Enterprise Identification
3	ESM_ICD.1	Identity and Credential Definition
4	ESM_ICT.1	Identity and Credential Transmission
5	FAU_STG_EXT.1	External Audit Trail Storage
6	FCS_TLS_EXT.1	TLS
7	FPT_APW_EXT.1	Protection of Stored Credentials
8	FPT_SKP_EXT.1	Protection of Secret Key Parameters

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.
  - **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".
  - **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold italics and are surrounded by brackets (e.g., *[**assignment**]**).***
  - **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**]).
  - **Refinement**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***<u>italicized bold and underlined text</u>***.

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

6.1.1 *Enterprise Security Management (ESM)*

6.1.1.1 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.

6.1.1.2 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.

6.1.1.3 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, ***[list of secret and template objects to which enterprise user has access to, type of access].***

Application Note: Internal Secret and Template attributes specified in the table below:

Table 13: Secret and Template Security Attributes

Object	Attribute
Secret	Secret Name
	Subject Identifier
	Field Data
	Folder[3]
	Policy Identifier
	Attributes Inherited from Template
	Password Requirements Rule Override
	Command Restrictions
Template[4]	Template Name
	Template Description
	Template Status
	Secret Expiration Policy

[3] Note: Folders are used to form groups of secrets, this attribute is functional equivalent to group membership.

[4] Note: Template is not an individual object, rather a predefined set of attributes used when creating a new object.

Object	Attribute
	Secret Name Pattern
	Field Parameters (Username, Password, Type)
	Secret Modification Policy
	Secret Access Policy
	Password Change Policy
	Password Strength Policy

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: ***[ASCII, Unicode UTF-8, and Unicode UTF-16]*** that include the following values ***[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;

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.

6.1.1.4 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: **[at a periodic interval, *[when requested by an authorized TOE user]*]**.

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_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)
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

Component	Auditable Events	Additional Audit Record Contents
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
FTA_TSE.1	Denial of session establishment	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

FIA_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]***.

FIA_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]***.

FIA_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: ***[user is associated with the assigned role immediately following authentication to the TSF]***.

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_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
	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

Requirement	Management 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
FTA_TSE.1	Management of session establishment conditions
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.1.1E	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:

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

7.1 Enterprise Security Management

7.1.1 *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.

7.1.2 *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 extends the identity of enrolled enterprise users to provide audited access to Enterprise IT assets (e.g. database server) that will in turn consume this identity data.

The TOE, Thycotic Secret Server Government Edition v10.1, integrates with a domain controller and then, based on individual or group identities offers access to specific IT assets or groups of IT assets within the enterprise environment. The TOE is capable of utilizing both existing logins, and generating and automatically rotating strong passwords that it assigns to IT assets. These logins are internally represented by objects called Secrets. The TOE synchronizes with Active Directory (AD) and can use both individual and group membership to grant access to Secrets. Additionally, the TOE is capable of creating and managing local users independently from AD.

The TOE facilitates access to the enterprise products that are not capable of directly integrating with domain controllers. The TOE enables authenticated users to remotely access compatible IT assets by using managed credentials via an integrated Putty Launcher or RDP Launcher.

The TOE integrates with a domain controller (i.e. Active Directory). Once integrated, the TOE can use domain group membership to control access to individual Secrets or groups (folders) of Secrets.

The TOE maintains two types of objects internally: Secrets and Secret Templates. Template can be used to create multiple unique Secrets, any Secret can have only one Template, and Templates are used to define most attributes in the Secret. Each Secret inherits attributes of corresponding Secret Template. For example, user name and password in a Unix Account (SSH) Secret are Field Data based on Field Parameters that are defined by Unix Account (SSH) Template. Field Data is the only attribute that is transmitted by the TOE to ESM products. Secrets do not have any other attributes, inherited or otherwise, that are transmitted to ESM products. Templates are fully internal objects, while Secrets are external-facing.

The purpose of a Secret is to describe and to enable control of a particular IT asset via policies. Attributes of these objects, among other things, contain the credentials to access a particular enterprise IT asset. When the TOE transmits credentials to managed IT assets, this data takes the form of a user name, password and optionally non-password based credentials such as RSA keys: all of which correspond to ‘Field Data’ attributes. Secrets are opaque from the point of view of TOE non-administrative users; their internal structure defined in the following table:

Table 25: Detailed Object Descriptions

Object	Attribute	Description	Transmitted to ESM products?
Secret	Secret Name	The secret name is the label or title that describes the content of each secret.	No
	Subject Identifier	The secret template of each secret identifies the type of store password or other data. This allows users to see the intended usage of each object.	No
	Field Data	Each attribute field in a secret is either “Text” “Password” or “Notes”. This attribute corresponds to Field Parameters in the Template object and contains specific values of user names, passwords, and optionally RSA keys.	Yes
	Folder	Folders are used to form groups of secrets, this attribute is functional equivalent to group membership.	No
	Policy Identifier	Secret policies are a collection of security and password settings that are applied to individual secrets or folders. Each setting of a secret policy can be configured as either	No

Object	Attribute	Description	Transmitted to ESM products?
		default or enforced. Default allows users to later change the setting. Enforced locks the settings and cannot be modified on a per-secret basis unless the secret is moved out of the folder that has the secret policy attached. Secret policy settings include items such as "Remote Password Changing Auto Change," and "Requires Approval for Access."	
	Attributes Inherited from Template	Secret templates dictate the fields each secret contains, the launchers for each secret, and the remote password changer used.	No
	Password Requirements Rule Override	A flag whether the password requirements are enforced or indicated via a warning. If password requirements are enforced, users cannot input the new password until it meets the requirements.	No
	Command Restrictions	Command restrictions are limited to SSH sessions and allow administrators to create multiple-choice command menus that users can follow. If SSH command menus are enabled, users cannot issue commands directly to the target system.	No
Template[5]	Template Name	The label that describes the type of Template. Only Windows Account, Active Directory Account, and Unix Account (SSH) templates were evaluated.	No
	Template Description	This field allows administrators to describe the purpose of a template when they create a new template, which is a recommended practice to organize multiple templates.	No
	Template Status	Administrators can disable individual templates to make them invisible to users. The status is either "enabled" or "disabled."	No
	Secret Expiration Policy	When a secret reaches its expiration date, it is flagged as "Expired." If automatic password rotation is enabled for that secret, expiration triggers a remote password change.	No
	Secret Name Pattern	When Secret Server names a secret via the discovery import process, it	No

[5] Note: Template is not an individual object, rather a predefined set of attributes used when creating a new object.

Object	Attribute	Description	Transmitted to ESM products?
		uses the naming convention "hostname/username," or "domain/username." Automatic account discovery was not evaluated.	
	Field Parameters (Username, Password, Type)	Field parameters include username, password, and optionally non-password based credentials of each Secret. Templates include a combination of field parameters that vary and are inherited by Secrets.	Yes
	Secret Modification Policy	Each secret carries individual access permissions that are typically inherited from the secret's folder. These permissions determine not only which users can view the secret but also which users are can edit the secret's data. A user can have view, edit, or owner permission.	No
	Secret Access Policy	If users have view (or greater) rights, they can see whether a secret exists and can open the secret to view its data. If a user does not have view rights, the secret is invisible.	No
	Password Change Policy	Password rotation is enabled or disabled on a per-secret or per-template basis. Password rotation frequency depends entirely on the expiration period for each secret.	No
	Password Strength Policy	A password policy is a set of rules governing how each new password is created.	No

There are four types of object access permissions:

- owner
- edit
- view
- list

These access permissions are granted to TOE users, or groups of TOE users, to regulate access to Secrets and to control access to managed IT assets. TOE users with the owner permission for a specific Secret have full control over that object and its access lists. All other categories offer less control, with list permission only allowing a user to see a list of Secrets in a specific Folder. The owner, edit, and view access permissions can be applied to individual Secrets or groups of secrets (called Folders). When an individual Secret belongs to a specific Folder it uses the access permission rules assigned to that specific Folder. A Secret can belong only to one Folder at a time, but a Folder can contain multiple Secrets.

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

The TOE can manage any IT asset compatible with the following types of credentials:

- Windows Account
- Active Directory Account
- Unix Account (SSH)

These credential types define a broad range of compatible ESM products. Generally, any modern system that supports a specific set of credentials and allows an operator to SSH or RDP into the system is supported. Specifically, Linux 2.6.32 or later, Windows Server 2008 R2 or later, Windows 7 Enterprise or later are compatible.

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 and are considered secure. 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 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.

7.1.3 *ESM_ICT.1*

The TOE extends the identity of enrolled enterprise users, with the identity extension taking the form of an object called a Secret. These objects contain the credentials to access a particular enterprise IT asset. Secrets are consumed by a specific enterprise IT asset at the time when an authenticated TOE user utilizes the TOE to access that specific IT asset.

The TOE also implements remote password change functionality that enables administrators to initiate a password change. This password change could be an immediate action, a scheduled one-time action, or a periodic automatic rotation. The periodic automatic password rotation is based on an administrator-configured schedule, periodically expiring existing credentials and triggering password rotations at predetermined intervals.

During password rotation, both the old credential data (to access an IT asset) and new credential data (as part of credential update) are securely transmitted. Each update takes effect immediately following the transmission of the modified credential data by the TOE to the managed IT asset. In the evaluated configuration, the automatic password change functionality is limited to a Unix Account (SSH), Windows Account, and an Active Directory Account. Unix Account (SSH) is secured using Secure Shell (SSHv2) protocol, Windows

Account and Active Directory Account are secured using Windows Remote Desktop (RDP) that is based on TLS protocol.

Internally, credential data used to access IT assets is stored as part of an object called a Secret. Secrets are opaque from the point of view of non-administrative TOE users; the structure of a Secret is defined in the Table 13: Secret and Template Security Attributes. When the TOE transmits ESM data to managed IT assets, this data takes the form of a user name, password and optionally non-password based credentials such as RSA keys: all of which correspond to ‘Field Data’ in Secret attributes.

The TOE also supports the Secure LDAP (LDAPS) protocol for communication with a compatible domain authentication server (Active Directory). The LDAP protocol is described in RFC 4510, and LDAPS is LDAP encapsulated in the TLS protocol (RFC 5246, RFC 4346).

Synchronization with Active Directory (AD) is periodic, with an administrator-configurable polling period. During synchronization the TOE connects to AD and sends a search request query (LDAP search operation) on the relevant domain group that the TOE includes in the search scope. In response, the AD will identify any entries within the specified scope and return a response (LDAP search result) to the TOE that includes the DNs of the matching entries along with the attributes contained in each entry. These responses will contain the CN and security group memberships that the TOE will in turn process to determine access of individual domain users to individual or group of Secrets. The TOE will synchronize with any configured domain within AD. When a new domain user is enrolled and joins a security group recognized by the TOE, the TOE will automatically import the user's attributes and determine user’s role and access permissions without any additional configuration steps performed by the TOE administrator.

7.2 Security Audit

7.2.1 *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 the Windows Event Logs (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. Remote logging utilizes syslog protocol (RFC 5242), with individual records varying depending on the message type, but in general containing timestamp, subject ID, event type, and the outcome message.

7.2.2 *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 2016 Standard Edition 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

7.3.1 *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 protocol is implemented by the operational environment, specifically Windows Server 2016 Standard Edition Secure Channel (`schannel`). The entirety of protocol operation, including all cryptographic operations (e.g., encryption and decryption), including extensions processing, including performing authentication, are implemented by the operational environment.

The TOE acts as a TLS server and authenticates itself with an X.509v3 certificate when remote administrators connect to it. The TOE acts as a TLS client when connecting to an external audit server, a typical audit server authenticates incoming connections based on the port and optionally the source IP address. The TOE acts as a TLS client when connection to an AD server, whereby the TOE authenticates itself with a username and passwords that are associated with a domain administrative account.

7.4 Identification and Authentication

7.4.1 *FIA_USB.1*

The TOE associates all of a user's security attributes with the subjects acting on the behalf of that user. Users receive their privileges either directly from the TOE or by way of membership in groups and/or roles (i.e. the TOE associates access to Secrets with the user's group memberships within a directory system agent such as Active Directory). The TOE implements RBAC, with any user assigned to an Administrator role considered a TOE administrator. Role assignments are separate from Secret access permissions, as described in Section 7.1.2. The TOE maintains the following default roles: Read-only, User, Administrator.

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

The user's attributes are tracked against the user's current logged-in session as maintained by the TOE. Attribute changes made for a user via the TOE are immediate, and therefore take effect immediately during the user's current active session, if the user is in fact logged in via the TOE to access an IT asset. These attributes are constantly checked with every action a user takes during their active session, i.e. accessing folders, secrets, performing administrative functions, etc.

7.4.2 *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

7.5.1 *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.

7.5.2 *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.

7.5.3 *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.

7.5.4 *FMT_MTD.1*

The local authentication data repository is implemented as a table in the Microsoft SQL Server installed locally in the operational environment (on the same hardware, on the same OS).

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 TSF

7.6.1 *FPT_APW_EXT.1*

The TOE is not directly responsible for storing authentication data. Instead it relies on the Operational Environment to encrypt all authentication data. Both local administrator authentication data and Secrets are stored in an encrypted table in the database. The database is in turn protected by an Access Control List (ACL) enforced by Windows Server 2016. Additionally, when local login-related authentication data is entered through regular TOE interfaces, it is obfuscated by substituting the entered data with a series of asterisks. The claimed Protection Profile do not require a specific method of obfuscation and the TOE does not directly control the process; however, Windows Server 2016 documentation states that it utilizes 256-bit AES encryption.

7.6.2 *FPT_SKP_EXT.1*

The TOE's client X.509v3 certificates and their associated private keys are protected by the Windows Server 2016 Access Control List (ACL) and Data Protection API (DPAPI). DPAPI is a built-in component of Windows Server 2016 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 2016 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

7.7.1 *FTA_TAB.1*

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

7.7.2 *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.

7.7.3 *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.

7.7.4 *FTA_TSE.1*

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

7.8 Trusted Path/Channels

7.8.1 *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 2016 Standard Edition to provide protocol and cryptographic functionality. Windows Server 2016 Standard Edition implements a FIPS certified (CMVP #2937) Cryptographic Primitives Library (bcrypt) that is also component validated for TLS key derivation. See Table 26: 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 26: TOE Certified Cryptography

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

Cryptographic Operation	Implementation	Certificate
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

Acronyms and Terminology

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

Table 27: Acronyms and Terminology

	Definition
CC	Common Criteria
CSP	Critical Security Parameter
Enrolled User	An enterprise user with valid domain credentials
EVT	Windows Event Log (EVT) format is used by Microsoft Windows to store audit information
FIPS	Federal Information Processing Standard
Folder	Folders are used to form groups of secrets, this attribute is a functional equivalent to group membership
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
Secret	Internal object that contains credentials to access a particular enterprise IT entity
SFR	Security Functional Requirement
ST	Security Target
Template	A predefined set of attributes used when creating a new secret
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface