Assurance Activity Report
for
Thycotic Secret Server Government Edition, Version 10.0

Version v1.7
10/23/2018

Produced by:

Prepared for:

Canadian Common Criteria Scheme (CCCS) and
Common Criteria Evaluation and Validation Scheme (CCEVS)

Thycotic Secret Server Government Edition, Version 10.0
Assurance Activity Report

Thycotic Secret Server Government Edition, Version 10.0
Assurance Activity Report

The Developer of the TOE:
Thycotic

The Security Target was developed by:
Cygnacom Solutions Inc.
1000 Innovation Drive Kanata, ON K2K 3E7¨Canada

The TOE Evaluation was sponsored by:
Thycotic
1191 17th Street NW, Suite 1102
Washington DC 20036

Table of Contents

Table of Tables

Table of Figures

1 Introduction

This document summarizes the evaluation results of a specific Target of Evaluation (TOE), Thycotic Secret Server Government Edition, Version 10.0, build 104.000003 conforming to Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, October 24, 2013, by listing the assurance activities and associated results as performed by the evaluators.

1.1 References

The following table provides information needed to identify and to control the Security Target (ST), the Target of Evaluation (TOE), and other evidence used in this evaluation.

Item	Identifier	Short Form
Security Target	Thycotic Secret Server Security Target v1.5	[ST]
Protection Profile	Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, October 24, 2013	[PP]
User Guidance	Common Criteria Hardening Guide, Secret Server v10.0, document version 1.011, August 2018	[ADMIN]
	Secret Server User Guide v1.1, July 2018	[ADMIN_USER]
	Secret server – Getting Started Guide v1.1, July, 2012	[ADMIN_STARTED]
Test Report	Thycotic Secret Server Government Edition Test Report v3.5	[TR]
Function specification document	Thycotic Secret Server Functional Specification ADV_FSP v0.3	[FSP]

Table 1: Guidance and Reference Documents

1.2 Target of Evaluation

The TOE, Thycotic Secret Server Government Edition, Version 10.0, build 104.000003 is 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.

1.2.1 *TOE Platform Requirements*

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

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.

1.2.2 *TOE equivalence*

Thycotic confirms that the platforms listed in the Table 2 are supported.

Table 2: Supported Platforms

Software	Platforms
Secret Server Government Edition v10.0, build 104.000003	Microsoft Windows Server 2012 R2 (x64) running on an Intel Core i7 with AES-NI
	Microsoft Windows Server 2012 R2 (x64) running on an Intel Core i5 with AES-NI
	Microsoft Windows Server 2012 R2 (x64) running on an Intel Xeon E5 with AES-NI

1.2.3 *Tested Platforms*

Testing was conducted using the TOE installed on Windows server 2012 R2 running on an Intel Xeon E5 with AES-NI on a physical hardware of Dell PowerEdge R710.

1.2.4 *Testing topology*

The topology (Figure 1) is configured for a dedicated 'Test' LAN for CC testing. This LAN is physically isolated via a dedicated core switch, preventing general access while still granting testers direct access to the TOE. The setup consists of a 'Test' LAN – 192.168.0.x for IPv4, a TOE installed in a physical server Dell PowerEdge R710, and a VMware Vsphere v5.6 server hosting an AD server, syslog, CA/CRL servers and a Linux system used as an access control server. A packet capture is done by a laptop connected to a mirrored port on the switch.

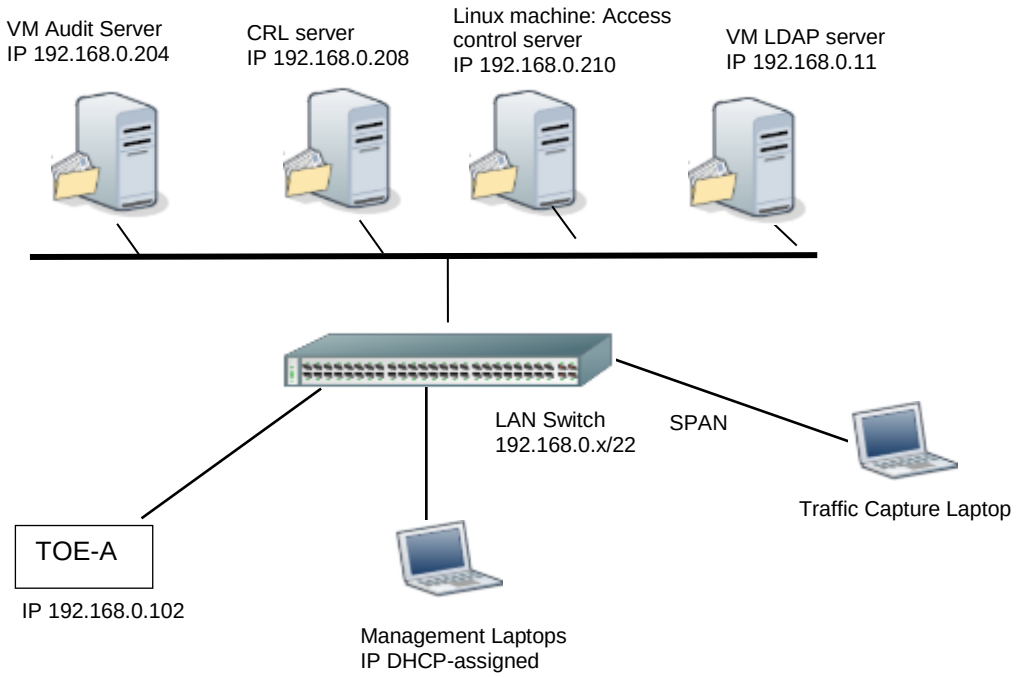

Figure 1: Network Topology

2 Security Functional Requirements

2.1 Enterprise Security Management (ESM)

2.1.1 *ESM_ATD.1 Object Attribute Definition*

2.1.1.1 TSS Assurance Activities

TSS Assurance Activities: *(1) The evaluator shall check the TSS to ensure that it describes the object attributes that are defined by the TOE and the purpose for their definition.*
TSS Implementation Details/Results: (1) The ST, Section 7.1, states that the 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.

2.1.1.2 Guidance Assurance Activities

Guidance Assurance Activities: *The evaluator shall check the operational guidance to ensure that it provides instructions on how to define and configure the object attributes.*
Guidance Implementation Details/Results: The ADMIN, Section 10 states that secret templates are used to create secrets and define object attributes for secrets. The Secret Templates is a defined list of pre-configured Secret Templates, however, Secret Server provides the ability to define new Secret Templates. The following is a list of Secret Templates that are compliant with Common Criteria standards available in the Government edition of Secret Server: ▪ Active Directory Account ▪ Bank Account ▪ Combination Lock ▪ Contact ▪ Pin ▪ Product License Key ▪ Security Alarm Code ▪ Credit Card ▪ Unix Account (SSH Key Rotation) ▪ Social Security Number Users only can create Secrets using templates marked as Active. To create new Secrets, users first choose a Secret Template, after that user needs to fill out the mandatory object attributes and save the new Secret. The Secret attributes vary from Secret Template to another. Section 10.1 describes the concepts of Secrets Templates and provides instructions on how these templates are used to create Secrets. Section 10.1 also lists objects attributes for both Secrets and Secret Templates.

2.1.1.3 Testing Assurance Activities

Testing Assurance Activities: *The evaluator shall test this capability by using a Policy Management product to create an access control policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy.*
Testing Implementation Details/Results: The evaluator created the following secrets: unix ssh Secret and an active directory Secret and shared both secrets and observed that the secrets can be accessed by the access control product.

2.1.2 *ESM_EAU.2 Reliance on Enterprise Authentication*

2.1.2.1 TSS Assurance Activities

TSS Assurance Activities: *The evaluator shall check the TSS in order to determine that it (1) describes the TSF as requiring authentication to use and (2) that it describes, for each type of user or IT entity that authenticates to the TOE, the identification and authentication mechanism that is used. (3)The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each authentication mechanism that is used by the TSF.*
TSS Implementation Details/Results: (1) The ST, Section 7.1 states that the TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. (2) The ST, Section 7.1 states The TOE users authenticate either locally using direct login, or remotely via a configured domain controller (in this case Active Directory). (3) The ST, Section 6.1.1.2 includes one instance of ESM_EAU.2 SFR, as iteration is unnecessary to describe the underlying SF.

2.1.2.2 Guidance Assurance Activities

Guidance Assurance Activities: *The evaluator shall (1) check the operational guidance in order to determine how the TOE determines whether an interactive user requesting access to it has been authenticated and (2) how the TOE validates authentication credentials or identity assertions that it receives.* *If any IT entities authenticate to the TOE, the evaluator shall also check the operational guidance to (3) verify that it identifies how these entities are authenticated and (4) what configuration steps must be performed in order to set up the authentication.*
Guidance Implementation Details/Results: (1) The ADMIN, Section 5 and noted that it adequately describes all authentication methods. The TOE can use local account and/or Active Directory for authentication with Secret Server. (2) The ADMIN. Section 5.1 details the process of authenticating a local user. The user must provide a username and password in order to login locally. The ADMIN, Section 5.2 details the process of authentication using Active directory. 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 (3) & (4) There are no IT entities that authenticate to the TOE.

2.1.2.3 Testing Assurance Activities

Testing Assurance Activities: *The evaluator shall* *(1) test this capability [Enterprise Authentication] by accessing the TOE without having provided valid identification and authentication information and observe that access to the TSF is subsequently denied. (2) If any IT entities authenticate to the TOE, the evaluator shall instruct these IT entities to provide invalid identification and authentication information and observe that they are not able to access the TSF.*
Testing Implementation Details/Results: (1) The evaluator provided an invalid local login and observed that the access is denied. The evaluator provided an invalid domain login and observed that the access is denied. (2) The evaluator misconfigured an active directory server to authenticate with an invalid certificate and observed that the connection was refused. The evaluator then misconfigured an audit server and

observed similar results.

2.1.3 *ESM_EID.1 Reliance on Enterprise Identification*

2.1.3.1 Assurance Activities

Assurance Activities:
This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2.

2.1.4 *ESM_ICD.1 Identity and Credential Definition*

2.1.4.1 TSS Assurance Activities

TSS Assurance Activities:

(1) The evaluator shall review the TSS to verify that it identifies compatible ESM products and describes the identity and credential data that are used by those products.

(2) The evaluator shall review public documentation for compatible products and verify that they actually use the data in the compatible way asserted by the TSS.

TSS Implementation Details/Results:

(1) The ST, Section 7.1, identifies the compatible ESM product as being Active Directory, which allows users to use their domain credentials to authenticate to the TOE. 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. The TOE also offers the capability to randomly generate strong passwords.

(2) The evaluator reviewed public documentation for Active Directory and verified that it actually uses authentication data in the compatible way asserted by the TSS. Active Directory also stores information about network components. Evaluator used the following public documentation: https://msdn.microsoft.com/en-us/library/bb742424.aspx#XSLTsection122121120120. During testing, the evaluator configured Microsoft Active Directory “doom.priv” domain and observed that the TOE successfully synchronize with it and concluded that the TOE use the data in the compatible way.

2.1.4.2 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall review the operational guidance in order to verify that it indicates how identity and credential data are supplied to the TOE and this data is identified.

With respect to the requirements regarding credential complexity: the evaluator shall examine the TSS and operational guidance in order to identify the form of credentials collected:

a. *For password-based credentials, the evaluator shall identify that all password composition, configuration, and aging requirements specified in the ST are discussed in the TSS and AGD and test these capabilities one at a time (for example: set minimum password length to 6, observe that a 7 character password and a 16 character password are both accepted, then change the minimum length to 8, observe that a 7 character password is rejected but that a 16 character password is accepted)*

b. *For non-password based credentials, the evaluator shall perform a basic strength of function analysis to determine the solution space of the authentication mechanism and the frequency with which password attempts can be made. For example, if the authentication is a 4-digit PIN that can*

be attempted once an hour, this requirement would not pass. If the strength of the authentication mechanism can't be determined by strength of function metrics at face value (for example, if a biometric authentication mechanism is being used), the vendor shall provide some evidence of the strength of function.

Guidance Implementation Details/Results:

(a) The ADMIN, Section 9.1 and noted that they clearly state what identity and credential data are generated by the TOE. Section 9.3 states that that passwords must be minimum 16 characters and include any of the following requirements:

- Upper case letters
- Lower case letters
- Numbers
- Special Characters: ! @ # $ % ^ & * ( )

(b) The AA is not applicable, as the TOE does not use non-password based credentials.

2.1.4.3 Testing Assurance Activities

Testing Assurance Activities:

(1) The evaluator shall test this [identity and credential data] capability by using the TOE to create identity and credential data and sending this data to the compatible ESM product(s) for consumption.

(2) These tests shall exercise each capability described in the SFR, including the ability to enforce credential complexity requirements. The evaluator will then perform basic identity and credential-related actions on the compatible ESM products that use the identity and credential data in order to confirm that the data was applied appropriately.

(3) For password-based credentials, the evaluator shall identify that all password composition, configuration, and aging requirements specified in the ST are discussed in the TSS and AGD and test these capabilities one at a time (for example: set minimum password length to 6, observe that a 7 character password and a 16 character password are both accepted, then change the minimum length to 8, observe that a 7 character password is rejected but that a 16 character password is accepted)

(4) For non-password based credentials, the evaluator shall perform a basic strength of function analysis to determine the solution space of the authentication mechanism and the frequency with which password attempts can be made. For example, if the authentication is a 4-digit PIN that can be attempted once an hour, this requirement would not pass. If the strength of the authentication mechanism can't be determined by strength of function metrics at face value (for example, if a biometric authentication mechanism is being used), the vendor shall provide some evidence of the strength of function.

Testing Implementation Details/Results:

(1) The evaluator created multiple secrets based on “Active directory Account” and “Unix Account (SSH)” Secret Templates and used corresponding Launcher to access corresponding IT entities. Based on successful access the administrator concluded that the TOE transmitted this data to the compatible ESM products for consumption. The evaluator also utilized automatic password change feature, observed successful password change as confirmed by a rejected manual attempt to use old password, and concluded that the TOE created identity and credential data for consumption by the compatible ESM products."

(2) During the creation of a secret, the evaluator had the chance to auto-generate a password or to enter it manually. During testing, the evaluator tested the enforcement of password complexity rules for manual passwords on the secrets, by entering password that confirms to the password complexity requirements and found it accepted, and by entering passwords, that it does not follow the password complexity requirements and found it get refused. For the auto-generated passwords on the secrets, Evaluator auto-generated passwords for different password requirements rules and found that the auto-generated passwords do confirm to the new password complexity requirements every time he setup a new one.

(3) For password-based credentials, the evaluator tested policy enforcement for auto-generated and

manually-generated passwords: character set, minimum length, password composition – special characters, password composition – numbers, password reuse. (4) For non-password based credentials: The evaluator instructed the SFR to generate an RSA key of 2048 bits size and used the RSA key in an SSH account secret type.

2.1.5 *ESM_ICT.1 Identity and Credential Transmission*

2.1.5.1 TSS Assurance Activities

TSS Assurance Activities: *(1)The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s).* *(2) The evaluator shall also check the TSS to see that it describes the ESM data that the TSF transmits to other ESM products and the circumstances that cause it to be transmitted.*
TSS Implementation Details/Results: (1) The ST, Section 7.1 claims that identity and credential data is transmitted immediately following modification of credential data (Secret) by the TOE, which is consistent with the ST, Section 6.1.1.5 (2) The ST, Section 7.1 states that 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.

2.1.5.2 Guidance Assurance Activities

Guidance Assurance Activities: *The evaluator shall review the operational guidance to determine how to create and update identity, credential (and potentially object attribute) data, and the circumstances under which new or updated data are transmitted to consuming ESM products (and how those circumstances are managed, if applicable).*
Guidance Implementation Details/Results: The ADMIN, Section 7.1 states that Active Directory Sync in Secret Server targets user account credentials from Active Directory. Secret Server will categorize users according to group information from Active Directory, but Secret Server does not create, delete, or alter Active Directory Group Policies. The synchronization is automatic with Active Directory.

2.1.5.3 Testing Assurance Activities

Testing Assurance Activities:

(1)The evaluator shall test this capability by obtaining the compatible ESM products. Following the procedures in the operational guidance for both the ICM and other ESM products, the evaluator shall create the indicated data (i.e., identity, credential, and potentially object attribute data) and ensure that the defined data is transmitted and installed successfully in compatible ESM products, in accordance with the circumstances defined in the SFR. In other words, (a) if the selection is completed to transmit after creation of new data, then the evaluator shall create the new data and ensure that, after a reasonable window for transmission, the new data is installed; (b) if the selection is completed to transmit periodically, the evaluator shall create the new data, wait until the periodic period has passed, and then confirm that the new data is present in the appropriate ESM components; or (c) if the section is completed to transmit upon the request of a compatible Secure Configuration Management component, the evaluator shall create the data, use the Secure Configuration Management component to request transmission, and the confirm that the appropriate ESM components have received and installed the data. If the ST author has specified "other circumstances", then a similar test shall be executed to confirm transmission under those circumstances.

(2)The evaluator shall then make a change to the previously created data, and then repeat the previous procedure to ensure that the updated data is transmitted to the compatible ESM components in accordance with the SFR-specified circumstances.

(3)Lastly, as updating data encompasses deletion of data, the evaluator shall repeat the process a third time, this time deleting the data to ensure it is removed as active data from the compatible ESM components.

Testing Implementation Details/Results:

(1) As part of the test case PP-6A: The evaluator configured an automatic password change on the credential (of the Secret) and observed an immediate transmission of the new password to the compatible ESM product. Evaluator used the new password and confirmed a successful access to the compatible ESM product.

(2) As part of the test case PP-6A: the evaluator took note of the old and new password, and then reconfigured another password Change in the secret. Evaluator observed an immediate attempt from the TOE to change the password in the ESM compatible product. Evaluator confirmed a successful transmission of the new password. Evaluator tried the old password and the new password and confirmed that the old password is no longer valid.

(3) As part of the test case PP-6C: Delete domain account, observe periodic synchronization, confirm old credentials no longer work

2.2 Security Audit (FAU)

2.2.1 *FAU_GEN.1 Audit Data Generation*

2.2.1.1 TSS Assurance Activities

TSS Assurance Activities:
(1) The evaluator shall check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records.
TSS Implementation Details/Results:
(1) The ST, Section 7.2 states that any use of a management functions via the web interface, as well as relevant IT environment events, will be logged. 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.

2.2.1.2 Guidance Assurance Activities

Guidance Assurance Activities:
The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record. *Each audit record format type shall be covered, and shall include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3.* *The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event.*
Guidance Implementation Details/Results:
The evaluator checked the [ADMIN] document, Appendix A and ensured that it lists all of the auditable events, provide a description of the location of the audit records, a description of the content of each type of audit records, and samples of auditable events. The evaluator checked the [ADMIN] document, Appendix A and found that each record format type contains the required information. The evaluator checked the [FSP] document and found that the TOE implements a Web GUI administrative interface that supports all management functions and generates appropriate audit events. The full list of auditable events and guidance location is in the following table:

Component	Auditable Events	Guidance
ESM_ATD.1	Definition of object attributes	Appendix-A
	Association of attributes with objects	Appendix-A
ESM_EAU.2	All use of the authentication mechanism	Appendix-A
ESM_EID.2	Creation or modification of identity and credential data	Appendix-A

ESM_ICD.1	Creation and modification of identity and credential data.	Appendix-A
	Enrollment or modification of subject	Appendix-A
ESM_ICT.1	Transmission of identity and credential data (and object attributes, if applicable) to external processes or repositories	Appendix-A
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Appendix-A
FCS_TLS_EXT.1	Failure to establish a session, establishment/termination of a session	Appendix-A
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	Appendix-A
FMT_MOF.1	All modifications of TSF function behavior	Appendix-A
FMT_SMF.1	Use of the management functions	Appendix-A
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	Appendix-A
FTA_SSL.4	The termination of an interactive session.	Appendix-A
FTP_ITC.1	All use of trusted channel functions	Appendix-A
FTP_TRP.1	All attempted uses of the trusted path functions	Appendix-A

The following management functions were identified in the PP as security relevant. These functions are documented in the user guidance and noted to generate appropriate audit events:

Requirement	Management Functions	Guidance
ESM_ATD.1	Definition of object attributes	ADMIN section 10
	Association of attributes with objects	ADMIN section 10
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	ADMIN section 5.1 and 5.2
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	ADMIN section 9 and 11.3
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	ADMIN section 10.5
	Management of credential status	ADMIN section 10
	Enrollment of users into repository	ADMIN section 10
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed	ADMIN section 7.1
FAU_STG_EXT.1	Configuration of external audit storage location	ADMIN section 13.0
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	ADMIN section 5.3
	Management of actions to be taken in the event of an authentication failure	ADMIN section 5.3
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	ADMIN section 5.0
FMT_MOF.1	Management of sets of users that can interact with security functions	ADMIN section 6.0 and 7.0
FMT_SMR.1	Management of the users that belong to a particular role	ADMIN section 8.0
FTA_SSL.3	Configuration of the inactivity period for session termination	ADMIN section 5.5
FTA_TAB.1	Maintenance of the banner	ADMIN section 5.4

FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	ADMIN section 11.3
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	ADMIN section 3.0

As related to Security Audit, ADMIN Section 12.1 explains audit logging and the audit log format, and Appendix A maps audit records to individual SFRs.

During testing, the evaluator confirmed that the information in ADMIN is accurate, and the examples are representative of a typical scenario encountered by the end-users.

2.2.1.3 Testing Assurance Activities

Testing Assurance Activities:

The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST.

This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is defined, the corresponding audit record should correctly identify the policy that was defined.

Testing Implementation Details/Results:

The evaluation team confirmed as part of testing activities that appropriate audit records were generated, and that each audit record contained appropriate and accurate information. See table below for details:

Component	Auditable Events	Test Case
ESM_ATD.1	Definition of object attributes	PP-1A
	Association of attributes with objects	PP-1B
ESM_EAU.2	All use of the authentication mechanism	PP-2
ESM_EID.2	Creation or modification of identity and credential data	PP-2
ESM_ICD.1	Creation and modification of identity and credential data.	PP-3, PP-4A, PP-4B, PP-4C, PP-4D, PP-4E, PP-4F, PP-4G.
	Enrollment or modification of subject	Pp-4G, PP-5
ESM_ICT.1	Transmission of identity and credential data (and object attributes, if applicable) to external processes or repositories	PP-6A, PP-6B, PP-6C
FAU_GEN.1	Start-up and shutdown of the audit functions; All auditable events for the not specified level of audit;	PP-7
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	PP-7, PP-8
FCS_TLS_EXT.1	Failure to establish a session, establishment/termination of a session	PP-9A, PP-9B, PP-9C.
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	PP-10
FMT_MOF.1	All modifications of TSF function behavior	PP-12
FMT_SMF.1	Use of the management functions	PP-12

FTA_SMR.1	Modifications to the members of the management roles	PP-11A, PP-11B, PP-11C and PP-12
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	PP-14
FTA_SSL.4	The termination of an interactive session.	PP-16
FTP_ITC.1	All use of trusted channel functions	PP-18A, PP-18B
FTP_TRP.1	All attempted uses of the trusted path functions	PP-19

2.2.2 *FAU_STG_EXT.1 External Audit Trail Storage*

2.2.2.1 TSS Assurance Activities

TSS Assurance Activities:

(1) The evaluator shall check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit.

NOTE: TD0066: Clarification of FAU_STG_EXT.1 Requirement in ESM PPs have been applied.

TSS Implementation Details/Results:

(1) The ST, Section 7.2 states that the TOE stores audit data locally (in the operational environment) by utilizing the Windows Event Log (EVT) system. When remote logging is enabled, 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.

2.2.2.2 Guidance Assurance Activities

Guidance Assurance Activities from PP:

The evaluator shall check the operational and preparatory guidance in order to determine that they

(1) describe how to configure and use an external repository for audit storage.

(2) The evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established.

Guidance Implementation Details/Results:

(1) The Common Criteria Hardening Guide, Section 13 External Auditing, describes how to configure an external repository for audit storage. Section 13.2.2 Configuration Steps provides detailed steps for TOE configuration.

(2) The Common Criteria Hardening Guide, Section 13.1 Security – Connecting to External Audit Server, details that TOE supports TLS v1.1 or TLS v1.2 and external audit server is authenticated based on certificate chain and trusted CAs. The secure channel encapsulates the syslog protocol and is compatible with syslog-ng or any other audit server that implements this protocol. In cases when connection to the audit server is lost, the TOE will automatically reconnect and resend any missed messages.

2.2.2.3 Testing Assurance Activities

Testing Assurance Activities:
The evaluator shall test this function in conjunction with testing of FAU_GEN.1 by *(1) confirming that the same set of audit records are received by each of the configured audit destinations.* *(2) The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one.*
Testing Implementation Details/Results:
(1) *During Test the Evaluator setup the TOE to send event logs to an external syslog-ng server, generated audit event in the TOE local audit storage, and confirmed both remote and local audit trails contain the same event.* (2) *During testing, the evaluator interrupted syslog connection, generated audit events in the local audit trail, re-established connection of the TOE with the syslog server and confirmed that both remote and local trails are synchronized.*

2.3 Cryptographic Support (FCS)

2.3.1 *FCS_TLS_EXT.1 TLS*

2.3.1.1 TSS Assurance Activities

TSS Assurance Activities:

(1) The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics (e.g., extensions supported, client authentication supported) are specified, and the ciphersuites supported are specified as well.

(2) The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.

(3) The evaluator shall also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions.

(4) For the cryptographic functions that are provided by the Operational Environment, the evaluator shall perform the following activities:

a. Ensure the ST contains a list of representative platforms (hardware and software) compromising the operational environment.

b. Check the TSS to ensure it describes-for each platform identified in the ST-the interface(s) used by the TOE to invoke this functionality.

c. For each platform identified in the ST, check the OE documentation to ensure the interfaces identified in the previous step exist.

NOTE: TD0320: TLS ciphers in ESM PPs have been applied.

TSS Implementation Details/Results:

(1) The ST, Section 7.3 states that the TOE supports TLS v1.1 and TLS v1.2 with all claimed ciphers for use with 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

(2) The evaluator checked the ST, Section 7.2 to ensure that the ciphersuites specified are identical to those listed for this component.

(3) The ST, Section 7.3 states that the cryptographic primitives associated with the TLS protocol are implemented by the operational environment.

(4) a. The ST, Section 1.4.1.1 identifies the hardware platform requirements and Section 1.4.1.2 identifies the software platform requirements.

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

c. The evaluator verified the ADMIN guide to ensure that the interfaces are described correctly.

2.3.1.2 Guidance Assurance Activities

Guidance Assurance Activities: *The evaluator shall check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).*
Guidance Implementation Details/Results: The ADMIN, Section 2.3.2 indicates that during the installation of the software, the TLS ciphers can be chosen so that the TOE conforms to the list described in the ST, Section 7.3.

2.3.1.3 Testing Assurance Activities

Testing Assurance Activities: *The evaluator shall test this capability by establishing a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of a HTTPS session. It is sufficient to observe (on the wire) the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).*
Testing Implementation Details/Results: 1. During the testing activity, the evaluator reviewed the traffic capture of the communication between the TOE and the syslog server, between the TOE and the AD server, and during the web session to the TOE web Server, and observed a successful negotiation of each of the ciphersuites specified by the ST. 2. During testing, the evaluator configured or observed the TOE successfully establishing TLS connections using the below 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

2.4 Identification and Authentication (FIA)

2.4.1 *FIA_AFL.1 Authentication Failure Handling*

2.4.1.1 TSS Assurance Activities

TSS Assurance Activities:
(1) The evaluator shall check the TSS in order to determine that the authentication failure handling function is described in sufficient detail to affirm the SFR.
TSS Implementation Details/Results:
(1) The ST, Section 7.4 states that if a user repeatedly fails to authenticate, their account will be locked after an administrator-configurable number of unsuccessful authentication attempts. To unlock a user account, an administrator with the correct role permissions must log into the Secret Server, navigate to that user in the Administration menu, and unlock the user's account.

2.4.1.2 Guidance Assurance Activities

Guidance Assurance Activities:
The evaluator shall check the operational guidance to verify that a discussion on authentication failure handling is present and consistent with the representation in the Security Target.
Guidance Implementation Details/Results:
The ADMIN, Section 5.3, states that an account becomes inaccessible after a limited number of unsuccessful authentication attempts until an Administrator unlocks the user's account. This is consistent with ST, Section 7.4. This section contains instructions on how to setup up this attribute and the process of unlocking the account

2.4.1.3 Testing Assurance Activities

Testing Assurance Activities:
(1)The evaluator shall test this capability by using the authentication function of the TSF to deliberately enter incorrect credentials. The evaluator shall observe that the proper action occurs after a sufficient number of incorrect authentication attempts. *(2) The evaluator shall also use the TSF to reconfigure the threshold value in a manner consistent with operational guidance to verify that it can be changed.*
Testing Implementation Details/Results:
(1) Test1: in PP-10 the evaluator deliberately cause lockout, ensured that threshold works by using correct credentials after the unlock happens and observe these credentials rejected for the entire lockout period. (2) As part of the test case PP-10, the evaluator Changed the lockout threshold and confirm that new value works.

2.4.2 *FIA_USB.1 User-Subject Binding*

2.4.2.1 TSS Assurance Activities

TSS Assurance Activities:
(1) The evaluator shall check the TSS in order to determine that it describes the security attributes that are assigned to administrators and the means by which the administrator is associated with these attributes, both during initial assignment and when any changes are made to them.
TSS Implementation Details/Results:
(1) The ST, Section 7.4 states that the TOE associates all of a user's security attributes with the subjects that are 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 a user's security attributes with the subjects acting on the behalf of that user: 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. The ST, Section 7.4 states that attribute changes for a user 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.

2.4.2.2 Guidance Assurance Activities

Guidance Assurance Activities:
The evaluator shall check the operational guidance in order to verify that it describes the mechanism by which external data sources are invoked and mapped to user data that is controlled by the TSF.
Guidance Implementation Details/Results:
The evaluator reviewed ADMIN Section 7, and noted it describes the mechanism by which external data sources are invoked and mapped to user data.

2.4.2.3 Testing Assurance Activities

Testing Assurance Activities:
(1) The evaluator shall test this [User-Subject Binding] capability by configuring the TSF to accept user information from external sources as defined by the ST. The evaluator shall then perform authentication activities using these methods and validate that authentication is successful in each instance. *(2) Based on the defined privileges assigned to each of the subjects, the evaluator shall then perform various management tests in order to determine that the user authorizations are consistent with their externally-defined attributes and the configuration of the TSF's access control policy. For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to policy information, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF that they do not have write access to policy information. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and used in order to determine what the user is able to do.*
Testing Implementation Details/Results:
(1) The evaluator configured the TOE to accept logging users from an AD server, the evaluator created domain users and assigned them to a specific security group (PP-11A). Evaluator confirmed that domain users were able to successfully logging to the TOE webUI. (2) In Test case PP-11B, evaluator confirmed that administrative permissions setup on the domain and local users were enforced correctly for local and domain users after successful login.

2.5 Security Management (FMT)

2.5.1 *FMT_MTD.1 Management of TSF Data*

2.5.1.1 TSS Assurance Activities

TSS Assurance Activities:
(1) The evaluator shall review the TSS in order to determine the repository in which the authentication data used by the TOE is stored. *(2) The evaluator shall also determine how communications with this repository is secured.*
TSS Implementation Details/Results:
(1) The ST, Section 7.5 states that the local authentication data repository is implemented as a table in the Microsoft SQL Server that is installed in the operational environment. (2) The ST, Section 7.5 states that access to the data stored in the Microsoft SQL Server is secured with a local system account that is unique to the TOE. The operating system enforces database access permissions and prevents unauthorized access to the authentication data stored there.

2.5.1.2 Guidance Assurance Activities

Guidance Assurance Activities:
The evaluator shall review the operational guidance in order to determine that it includes the data that can be managed and who is able to manage this data. This can be separated over multiple roles to distinguish between user administration and self-service; for example, both a Security Administrator and a specific user may be able to modify that user's own password.
Guidance Implementation Details/Results: The ADMIN. Section 8.0 lists the following roles: • Administrator • User • Read Only User The ADMIN, Section 8.2 details all of the roles and their management functions.

2.5.1.3 Testing Assurance Activities

Testing Assurance Activities:
(1) *The evaluator shall test this capability by performing the identified management activities with authorized roles in order to determine that they are allowed.* (2) *The evaluator shall also attempt to perform these activities with unauthorized roles in order to determine that they are not allowed.* (3) *Finally, the evaluator shall verify that communications between the TSF and the authentication data repository are secured by repeating the testing for FTP_ITC.1 over the interface between the two components.*
Testing Implementation Details/Results: (1) Test 1: in PP-12, the evaluator assigned users to specific user roles, logged in to the TOE WebUI using those users accounts and confirmed that the users were allowed to perform the identified management activities specific to each role. (2) Test 2: in PP-11B, the evaluator confirmed that user accounts assigned to specific roles, were not allowed to carry certain management activities that are not allowed in the user role. (3) Test 3: in PP-18A, the evaluator observed that the TOE communications with the LDAP server over a

secured TLS channel.

2.5.2 *FMT_MOF.1 Management of Function Behavior*

2.5.2.1 TSS Assurance Activities

TSS Assurance Activities: *(1)The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s).* *(2)The evaluator shall also check the TSS to see that it describes the ability of the TSF to perform the required management functions and the authorizations that are required to do this.*
TSS Implementation Details/Results: (1) The evaluator verified Section 6.1.5.1 Management of Functions Behavior and determined that the assigments were completed in a manner that is consistent with Section 7.5. (2) The ST, Section 7.5 states the TOE restricts management functions to authorized administrators. An administrator will authenticate to the TOE by providing their local or domain user credentials. The ST, Section 6.1.5.1, Table 15: Roles and Management Functions list all management functions assigned for the user roles supported by the TOE.

2.5.2.2 Guidance Assurance Activities

Guidance Assurance Activities:
The evaluator shall review the operational guidance in order to determine what restrictions are in place on management of these attributes and how the TSF enforces them. For example, if management authority is role-based, then the operational guidance shall indicate this.

Guidance Implementation Details/Results:

The ADMIN, Section 8.2 describes how TOE restricts access to management functions based on roles.

The following table, based on ADMIN, Section 8.2 details management function and the authorized roles.

Requirement	Management Activities	Role
ESM_ATD.1	Definition of object attributes	Administrator
	Association of attributes with objects	Administrator
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Administrator
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Administrator
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	Administrator
	Management of credential status	Administrator
	Enrollment of users into repository	Administrator
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed	Administrator
FAU_STG_EXT.1	Configuration of external audit storage location	Administrator
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	Administrator
	Management of actions to be taken in the event of an authentication failure	Administrator
FIA_USB.1	Definition of default subject security attributes, modification of	Administrator

	subject security attributes	
FMT_MOF.1	Management of sets of users that can interact with security functions	Administrator
FMT_SMR.1	Management of the users that belong to a particular role	Administrator
FTA_SSL.3	Configuration of the inactivity period for session termination	Administrator
FTA_TAB.1	Maintenance of the banner	Administrator
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	Administrator
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	Administrator

2.5.2.3 Testing Assurance Activities

Testing Assurance Activities:

The evaluator shall test this function [Management Functions] by accessing the TSF using one or more appropriately privileged administrative accounts and determining that the management functions as described in the ST and operational guidance can be managed in a manner that is consistent with any instructions provided in the operational guidance. If the TSF can be configured by an authorized and compatible Secure Configuration Management product, the evaluator shall also configure such a product to manage the TSF and use this product to perform the defined management activities. In addition, any access restrictions to this behavior should be enforced in a manner that is consistent with the relevant documentation. The evaluator shall test this by attempting to perform a sampling of the available management functions using one or more unprivileged accounts to observe that the activities are rejected or unavailable.

Testing Implementation Details/Results:

Test 1: The evaluator performed (see test case PP-12) a representative subset of management functions using multiple roles and determined that they operate as described in the ST and guidance. It was determined that administrative accounts have appropriate permissions, non-administrative roles do not have access to management functions, and there is no obvious way to bypass access control measures implemented via web-based interface.

Test 2: Not applicable, as the TOE does not claim to be compatible with any secure configuration management products.

2.5.3 *FMT_SMF.1 Specification of Management Functions*

2.5.3.1 TSS Assurance Activities

TSS Assurance Activities:

(1) The evaluator shall check the TSS in order to determine that it summarizes the management functions that are available.

TSS Implementation Details/Results:

(1) The ST, Section 7.5 states that the Table 16: TOE management Functions identifier all the management functions that are implemented by the TOE

2.5.3.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall check the operational guidance in order to determine that it defines all of the management functions that can be performed against the TSF, how to perform them, and what they accomplish.

Guidance Implementation Details/Results:
The ADMIN, Section 8.2 Management Functions based on role, defines all of the management functions and the corresponding user roles. The ADMIN document describes how to perform those management functions and the outcome of every function perfumed by each role.

2.5.3.2 Testing Assurance Activities

Testing Assurance Activities:
The evaluator shall test this capability by accessing the TOE and verifying that all of the defined management functions exist, that they can be performed in the prescribed manner, and that they accomplish the documented capability.
Testing Implementation Details/Results:
During the whole testing activity the evaluator verified that he was able to perform all the management functions according to the prescribed manner.

2.5.4 *FMT_SMR.1 Security Management Roles*

2.5.4.1 TSS Assurance Activities

TSS Assurance Activities:
(1) The evaluator shall review the TSS to determine the roles that are defined for the TOE. *(2) The evaluator shall also review the TSS to verify that the roles defined by this SFR are consistently referenced when discussion how management authorizations are determined.*
TSS Implementation Details/Results:
(1) The ST, Section 7.5 states that the TOE maintains the following default roles: Read-only, User, Administrator. These roles are listed in **Error! Reference source not found.**. (2) The evaluator verified that roles defined in Section 6.1.5.4 Security Management Roles are consistent with Section 7.5 of the ST.

2.5.4.2 Guidance Assurance Activities

Guidance Assurance Activities:
The evaluator shall review the operational guidance in order to verify that it provides instructions on how to assign users to roles. If the TSF provides only a single role that is automatically assigned to all users, then the evaluator shall review the operational guidance to verify that this fact is asserted.
Guidance Implementation Details/Results:
The ADMIN, Section 8.0 Common Criteria Roles and Permissions, describes Administrator, User, Read Only User as roles that “comply with Common Criteria standards”. The ADMIN, Section 8.1 Assigning Roles to Users, describes how to assign users to roles.

2.5.4.3 Testing Assurance Activities

Testing Assurance Activities:
The evaluator shall test this capability by using the TOE in the manner prescribed by the operational guidance to associate different users with each of the available roles. If the TSF provides the capability to define additional roles, the evaluator shall create at least one new role and ensure that a user can be assigned to it. Since other assurance activities for management requirements involve the evaluator assuming different roles on the TOE, it is possible that these testing activities will be addressed in the

course of performing these other assurance activities.
Testing Implementation Details/Results: The evaluator created both local and domain users and assigned each of the claimed roles (Administrator, User, and Read-only) to these users and confirmed that role permissions were enforced. The TSF provided the capability to define additional roles, the evaluator created a custom role, assigned a user to this new role and confirmed that this assignment was successful.

2.6 Protection of the TSF (FPT)

2.6.1 *FPT_APW_EXT.1 Protection of Stored Credentials*

2.6.1.1 TSS Assurance Activities

TSS Assurance Activities:
(1) The evaluator shall examine the TSS to determine that it details all authentication data, other than private keys addressed by FPT_SKP_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the TOE to access services in the operational environment (such as might be found in stored scripts). *(2) (2) The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. Alternatively, if authentication data is not stored by the TOE because the authoritative repository for this data is in the Operational Environment, this shall be detailed in the TSS.*
TSS Implementation Details/Results:
(1) The ST, Section 7.6 states that the TOE protects authentication data, such as stored passwords, so it is not directly accessible in plaintext. Locally stored password information is obscured by use of AES256 encryption. (2) Authentication data are not stored in the clear as outlined in the application note. This was verified in the ST, Section 7.6.

2.6.1.2 Guidance Assurance Activities

Guidance Assurance Activities: None
Guidance Implementation Details/Results: N/A

2.6.1.3 Testing Assurance Activities

Testing Assurance Activities:
The evaluator shall test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to non-administrative users. The evaluator shall similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured and that the system is configured such that data is inaccessible to non-administrative users.
Testing Implementation Details/Results: The evaluator identified following credential repositories: SQL database. The evaluator examined how credentials uses to access database are protected (test case PP-15A) and determined that relevant configuration files are encrypted using platform functionality (DPAPI). The evaluator identified database tables that store credentials (test case PP-15B) and confirmed that all passwords are stored encrypted in the database, and that access to the database tables requires appropriate level of privilege. Combined, these test cases ensure that credential are stored obscure and that the repository are not accessible to non-administrative users. The evaluator analyzed product architecture and identified installation scripts as a potential source of stored or hard coded credentials. When inquired about these scripts, the vendor performed internal audit of

these scripts and affirmed that installation scripts do not contain credentials. The evaluator have not independently verified this claim

2.6.2 *FPT_SKP_EXT.1 Protection of Secret Key Parameters*

2.6.2.1 TSS Assurance Activities

TSS Assurance Activities:
(1) The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.
TSS Implementation Details/Results:
(1) The ST, Section 7.6 states that X.509v3 certificates and their associated private keys are stored in the Windows Server 2012 Certificate Store. Other secrets, when stored in non-volatile memory, are encrypted with the Master Key, which is in turn is protected by the Data Protection API (DPAPI). The operational environment implements both the Certificate Store and the DPAPI. The operational environment also implements all protocols and handles associated keys. The TOE does not implement a mechanism designed to circumvent these Windows Server 2012 features.

2.6.2.2 Guidance Assurance Activities

Guidance Assurance Activities:
There are no operational guidance activities for this SFR.
Guidance Implementation Details/Results: N/A

2.6.2.3 Testing Assurance Activities

Testing Assurance Activities:
There are no testing activities for this SFR.
Testing Implementation Details/Results: N/A

2.7 TOE Access (FTA)

2.7.1 *FTA_TAB.1 TOE Access Banner*

2.7.1.1 TSS Assurance Activities

TSS Assurance Activities: *The evaluator shall check the TSS in order to determine that it discusses the ability of the TSF to display a configurable banner prior to administrator authentication.*
TSS Implementation Details/Results: The ST, Section 7.7 states that the TOE can be configured to display administrator-configured advisory banners as part of the authentication prompt.

2.7.1.2 Guidance Assurance Activities

Guidance Assurance Activities: *The evaluator shall review the operational guidance to determine how the TOE banner is displayed and configured.*
Guidance Implementation Details/Results: The ADMIN, Section 5.4 and noted it describes how to configure the TOE banner and how to modify the messaging.

2.7.1.3 Testing Assurance Activities

Testing Assurance Activities: (1) *If the banner is not displayed by default, the evaluator shall configure the TOE in accordance with the operational guidance in order to enable its display. The evaluator shall then attempt to access the TOE and verify that a TOE banner exists.* (2) *If applicable, the evaluator will also attempt to use the functionality to modify the TOE access banner as per the standards defined in FMT_SMF.1 and verify that the TOE access banner is appropriately updated.*
Testing Implementation Details/Results: Test 1: going through the PP-13, the evaluator enabled the banner display, and confirmed that it get displayed correctly, whenever the user connects to the TOE WebUI interface. Test 2: going through the test case steps in the PP-13, the evaluator was able to modify the banner text and observed that the modification took place when he reconnected to the TOE WebUI interface.

2.7.2 *FTA_SSL.3 TSF-initiated Termination*

2.7.2.1 TSS Assurance Activities

TSS Assurance Activities: *The evaluator shall check the TSS in order to determine that it discusses how inactivity is handled for remote administrative sessions.*
TSS Implementation Details/Results: The ST, Section 7.7 states that the TOE can be configured by an administrator to force an interactive session timeout value (any positive integer value in minutes). 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 in order to establish a new session.

2.7.2.2 Guidance Assurance Activities

Guidance Assurance Activities:
The evaluator shall also check the operational guidance in order to verify that it describes how to set the idle time threshold.

Guidance Implementation Details/Results:
The ADMIN, Section 5.5 and verified that it describes how to set inactivity timer for remote administrative sessions.

2.7.2.3 Testing Assurance Activities

Testing Assurance Activities:
The evaluator shall test this capability by following the operational guidance to configure several different values for the inactivity time period referenced in the component; these shall consist at least of the minimum and maximum allowed values as specified in the operational guidance, as well as one other value. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.

Testing Implementation Details/Results:
Test 1: in the test case PP-14, the evaluator enabled the inactivity timeout, set it to 2, 3, 5 and 10 minutes , established a remote web session and observed that the sessions got terminated after the configured time period and forced enter the credential to login back to the TOE webUI.

2.7.3 *FTA_SSL.4 User-initiated Termination*

2.7.3.1 TSS Assurance Activities

TSS Assurance Activities:
The evaluator shall check the TSS in order to determine that it discusses the ability of an administrator to terminate their own session.

TSS Implementation Details/Results:
The ST, Section 7.7 states that any administrative session can be terminated by logging out. Once terminated, the user will be required to re-enter their user name and password to re-authenticate with the domain controller prior to establishing a new session.

2.7.3.2 Guidance Assurance Activities

Guidance Assurance Activities:
The evaluator shall check the operational guidance in order to verify that it describes how an administrator can terminate their own administrative session for each administrative interface that is supported by the TOE.

Guidance Implementation Details/Results:
The ADMIN, Section 3.2 details how an administrator can terminate their own administrative session by clicking on Logout button.

2.7.3.3 Testing Assurance Activities

Testing Assurance Activities: *The evaluator shall test this [User-initiated termination] capability by establishing a session with the TOE using an administrative interface. The evaluator then follows the operational guidance to exit or log off of the session and observes that the session has been terminated. If applicable, the evaluator shall repeat this test for each administrative interface that is supported by the TOE.*
Testing Implementation Details/Results: Test 1: the evaluator was able of establishing a secure session with the TOE using a WebUI interface, and that no further administrative actions are possible without authentication. The evaluator was able to log out of the WebUI interface and observed no further administrative actions are possible without re-authentication.

2.7.4 *FTA_TSE.1 TOE Session Establishment*

2.7.4.1 TSS Assurance Activities

TSS Assurance Activities: *The evaluator shall examine the TSS to determine that all of the attributes on which a session can be denied are specifically defined.*
TSS Implementation Details/Results: The ST, Section 7.7 states that the TOE can be configured to deny session establishment based on IP Address Range.

2.7.4.2 Guidance Assurance Activities

Guidance Assurance Activities: *The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS.*
Guidance Implementation Details/Results: The ADMIN, Section 5.6 details how to configure IP address restrictions.

2.7.4.3 Testing Assurance Activities

Testing Assurance Activities: *The evaluator shall test this capability by first fully establishing a session to the TOE. The evaluator then follows the operational guidance to configure the TOE so that that access is denied based on a specific value of the attribute. The evaluator shall then attempt to establish a session in contravention to the attribute setting (for instance, the location is denied based upon the time of day). The evaluator shall observe that the session establishment attempt fails.*
Testing Implementation Details/Results: Test 1: The evaluator configured the TOE to restrict access based on specific IP address, restricted a user login access based on a specific IP address and confirmed that users opening WebUI session from different IP address than the one configured in the TOE was not possible.

2.8 Trusted Path/Channels (FTP)

2.8.1 *FTP_ITC.1 Inter-TSF Trusted Channel*

2.8.1.1 TSS Assurance Activities

TSS Assurance Activities:

(1) The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity and the method of assured identification of the non-TSF endpoint.

(2) The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

NOTE: TD0245: Updates to FTP_ITC and FTP_TRP for ESM PPs have been applied.

TSS Implementation Details/Results:

(1) The ST, Section 7.8 states that 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 X.509v3 authentication.

(2) The evaluator confirmed with the ST, Section 7.8 and Section 6.1.8.1 that all specified protocols are included in both sections.

2.8.1.2 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

NOTE: TD0245: Updates to FTP_ITC and FTP_TRP for ESM PPs have been applied

Guidance Implementation Details/Results:

The ADMIN, Section 7.1.3 and noted it describes how to configure TLS for Active Directory.

The ADMIN, Section 13.3 and noted it describes how to configure TLS for Syslog.

2.8.1.3 Testing Assurance Activities

Testing Assurance Activities:

The evaluator shall perform the following tests:

Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities.

Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.

Test 4: The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted[HD1] [MS2] . The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected.

NOTE: TD0245: Updates to FTP_ITC and FTP_TRP for ESM PPs have been applied

Testing Implementation Details/Results:

Test 1: during test case PP-18A,B, the evaluator established TLS connections to syslog server and to the AD Server using valid and invalid certificates. The evaluator observed that the communications using good

certificates were successful, however the communications using invalid certificates were unsuccessful to bot the Syslog server and the AD server.

Test 2: The evaluator followed the ADMIN guide to setup secure communication via TLS for syslog and Active Directory successfully. The communications to syslog and AD using TLS were initiated from the TOE.

Test 3: during the test case PP-18x, for both the TOE's connections with the syslog and AD servers, the evaluator verified that the channels data were not sent in plaintext and Wireshark traffic capture files were used to verify that the data was indeed encrypted.

Test 4: The evaluated disrupted the connection to syslog server, and noted that upon restoring the connection the data was not sent in plaintext.

2.8.2 *FTP_TRP.1 Trusted Path*

2.8.2.1 TSS Assurance Activities

TSS Assurance Activities:

(1) The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity and the method of assured identification of the non-TSF endpoint.

(2) The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

NOTE: TD0245: Updates to FTP_ITC and FTP_TRP for ESM PPs have been applied.

TSS Implementation Details/Results:

(1) The ST, Section 7.8 states that the TOE utilizes the 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 X.509v3 server authentication.

(2) The ST, Section 7.8 states that the TOE utilizes Internet Information Services (IIS) web server to offer secure remote administration and is protected by TLS v1.1 or TLS v1.2 protocol.

2.8.2.2 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

NOTE: TD0245: Updates to FTP_ITC and FTP_TRP for ESM PPs have been

Guidance Implementation Details/Results:

The ADMIN, Section 11.3.3 and noted it describes how to configure TLS with IIS for remote administration of the TOE.

2.8.2.3 Testing Assurance Activities

Testing Assurance Activities:

The evaluator shall perform the following tests:

Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities.

Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the

channel data is not sent in plaintext. *Test 4: The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted[HD1] [MS2] . The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected.* *NOTE: TD0245: Updates to FTP_ITC and FTP_TRP for ESM PPs have been applied*
Testing Implementation Details/Results: Test 1: during the test case PP-19, evaluator was able to establish HTTPS/TLS with IIS to access the TOE's Web UI, and observed that the communication was successful. Test 2: during the PEN1 and PEN 2 test cases, the evaluator came to conclusion that there was no other administrative interfaces beside the https interface on port 443 open. Test 3: during the test case PP-19, the evaluator reviewed the captured traffic during the time of establishing the channel data for the remote administration of the Web UI and concluded that no data was send in plaintext. Test 4: The evaluated disrupted the connection to Syslog Server, and noted that upon restoring the TLS connection, the TLS connection was renegotiated, successfully re-established and the transmitted data was properly protected.

3 Security Assurance Activities

3.1.1 *ADV_FSP.1 Basic Functional Specification*

3.1.1.1 Assurance Activities

Assurance Activities:
(1) Note: 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.
Assurance Activities Details/Results:
(1) The evaluator verified the [FSP] document and determined that the various interfaces were explicitly defined. The evaluator was able to carry all the needed activities using the documented interfaces.

3.1.2 *AGD_OPE.1 Operational User Guidance*

3.1.2.1 Assurance Activities

Evidence Assurance Activities:
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.
Guidance Assurance Activities Details/Results:
The ADMIN, Section 11.1.2, details that the Secret Server Government Edition Installer checks for FIPS encryption security standards on the Windows local server and enables FIPS mode by default in Secret Server. The cryptographic functionality is provided by the operational environment so there are no other cryptographic engines that were evaluated.

3.1.3 *AGD_PRE.1 Preparative Procedures*

3.1.3.1 Assurance Activities

Evidence Assurance Activities:
(1) 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.
Evidence Assurance Activities Details/Results:
(1) The evaluator has determined that the combination of the ADMIN guide and ST and determined that the documents address all platforms claimed for the TOE in the ST. The TOE consists of the following platforms:

- 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
- Microsoft Windows Server 2012 R2 (x64) running on Intel Xeon E5 with AES-NI

**The vendor affirms that the TOE can successfully execute on all of the above platforms.*

3.1.4 *ALC_CMC.1 Labeling of the TOE*

3.1.4.1 Assurance Activities

Evidence Assurance Activities:

(1) 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.

(2) 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.

Evidence Assurance Activities Details/Results:

(1) The evaluator checked ST, Section 1.2 TOE Reference and it identifies the TOE as Thycotic Secret Server Government Edition, Version 10.0, build 104.000003

(2) The evaluator reviewed the provided AGD guidance and the TOE software installer received for testing and has confirmed the version number is consistent with what is in the ST document.

3.1.5 *ALC_CMS.1 TOE CM Coverage*

3.1.5.1 Assurance Activities

Evidence Assurance Activities:

(1) 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.

Evidence Assurance Activities Details/Results:

(1) The evaluator checked ST, Section 1.2 TOE Reference and the ADMIN guide, and they both identify the TOE as Thycotic Secret Server Government Edition, Version 10.0, build 104.000003.

3.1.6 *ATE_IND.1 Independent Testing - Conformance*

3.1.6.1 Assurance Activities

Assurance 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 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 evaluators shall 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 (that 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.

Assurance Activities Details/Results:

The Test Report v3.5 was supplied as part of the testing efforts. During testing activity, the TOE platform was installed in an isolated LAN, where it is communicating with a setup of servers, installed in VMware Vsphere v6.5 server. The Test Plan contained the platforms tested and documented all test cases dictated by the ESM ICM PP. the test plan contains 7 initial configuration tests cases (IT-1.0 to IT-1.6), 34 manual tests (PP-1x to PP-19) and 4 penetration tests case (PEN-1 to PEN-3). Each test case was performed and assigned a pass verdict resulting in overall pass verdict for the testing effort.

3.1.7 *AVA_VAN.1 Vulnerability Survey*

3.1.7.1 Assurance Activities

Testing Assurance 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.

Testing Assurance Activities Details/Results:

The evaluator performed searches on public information from the following sources:

- National Vulnerability Database (https://nvd.nist.gov)
- CVE details (https://www.cvedetails.com)
- vulners.com
- securityfocus.com

The evaluator requested the vendor to provide a comprehensive list of third-party components. Using this list identifying 333 libraries, toolkits, and components along with "Thycotic", "Secret Server", ".NET" search terms the evaluator performed public vulnerability search. The result of the search were 248 vulnerabilities

in total, in addition of the Vendor list, the evaluator went through all of them, and determined that most of them are not applicable or irrelevant, and reported the rest to the vendor, who replied with a rational for why the vulnerability is not irrelevant or applicable to the TOE.