Assurance Activity Report
For
Thycotic Secret Server Government Edition, Version 10.1

Version v0.9
12/18/2018

Produced by:

Prepared for:

National Information Assurance Partnership (NIAP)

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 10.1, 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 v2.4	[ST]
Protection Profile	Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, October 24, 2013	[PP]
Common Criteria Configuration Guide	Common Criteria Hardening Guide, Secret Server v10.1, document version 1.003, December 2018	[CC GUIDE]
User Guidance	Secret Server User Guide v1.1, July 2018	
	Secret server – Getting Started Guide v1.1, July, 2012	
Test Report	Thycotic Secret Server Government Edition Test Report v1.2	[TR]
Function specification document	Thycotic Secret Server Functional Specification ADV_FSP v0.4	[FSP]

Table 1: Guidance and Reference Documents

1.2 Target of Evaluation

The TOE, Thycotic Secret Server Government Edition, Version 10.1, build 104.000003 is an enterprise identity and credential management application. 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 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. Additionally, the TOE is capable of creating and managing local users independently from AD.

The TOE maintains two types of objects internally: Secrets and Secret Templates. These objects contain the credentials required to access a particular enterprise IT asset. Secrets are opaque from the point of view of TOE non-administrative users.
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. For example, a Unix Account (SSH) would allow managing CentOS-based server.

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, the TOE consists of the software application running on Microsoft Windows Server 2016 Standard Edition installed on platforms listed in the Table 2.

1.2.2 *TOE Equivalence*

The TOE, in the evaluated configuration, consists of the following:

Table 2: Supported Platforms

Software	Platforms
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

The following platform was selected for testing:

Software	Platforms
Secret Server Government Edition v10.1	Microsoft Windows Server 2016 Standard (x64) running on Intel Xeon E5 with AES-NI

Rationale for selection of platform for testing
The TOE is a .NET software application that runs on top of a host machine's operating system. The vendor specified the minimum software and hardware requirements in the ST Section 1.4.1.1 Table 2. These requirements can be understood as "anything that runs Microsoft Windows Server 2016 Standard (x64)". For lab testing purposes, the TOE was installed on a Dell PowerEdge R710 with an Intel Xeon E5 with AES-NI running Microsoft Windows Server 2016 Standard (x64). This setup meets the specified minimum requirements, covers the only claimed OS (Windows Server 2016 Standard (x64)) and matches one of the platforms claimed in the ST Section 1.2 Table 1. Therefore, this setup is both representative and suitable for testing the TOE.

Rationale for selection of compatible ESM products

Putty is a GUI tool that supports connections to remote hosts using SSH with a username and either a password or a private key. Putty connects to a remote system with the provided username to launch an SSH session, and either presents a previously-entered password (supplied by the operator) or the selected private key or prompts the operator to provide a password before the SSH session can be fully established. The ST claims Linux 2.6.32 or later as a compatible ESM product for Unix Account (SSH). The managed system used during testing was running CentOS 7, that meets this minimum requirement and is a commonly used enterprise Linux-based OS. Therefore, this setup is both representative and suitable for testing the TOE.

Remote Desktop launcher (RDP) supports opening a Windows session on a remote Windows host, and authenticates the user with privileged credentials provided by Secret Server. It works with both Active Directory and local Windows accounts, and supports logins to non-domain joined Windows servers. RDP connects to the remote Windows system with a username, prompts the operator to provide a password, then opens up a window that contains an active Windows session running on the remote Windows system. The ST claims Windows 7 Enterprise or later as a compatible ESM product for Windows Account, Active Directory Account. The managed system used during testing was running Windows 7 Enterprise (x64) that meets this minimum requirement and is a commonly used enterprise Windows-based OS. Therefore, this setup is both representative and suitable for testing the TOE.

1.2.3 *Tested Platforms*

Testing was conducted using the TOE installed on Microsoft Windows Server 2016 running on an Intel Xeon E5 with AES-NI on a physical hardware of Dell PowerEdge R710.

1.2.4 *Testing Topology*

The test topology is shown and described in Figure 1. Both the TOE and its test network / LAN were located in the Common Criteria lab, with all OE Servers and the TOE connected to an isolated 'Test' LAN that was dedicated to this project. This LAN is physically isolated via a core switch dedicated to testing and logically separated by a dedicated VLAN, preventing general access while still granting testers direct access to the TOE. The setup consists of a ‘Test’ LAN – 192.168.0.x/16 IPv4 network with all servers assigned static IPv4 addresses within that class. The TOE's IPv6 capability was not tested during the evaluation. The TOE was installed on a dedicated Dell PowerEdge R710 blade server. Other OE servers were installed in Virtual Machines (VMs) running on a VMware VSphere v6.5 server and included: AD, syslog, and CA/CRL servers and CentOS 7 and Windows 7 managed VMs. Packet capture was performed using a dedicated laptop connected to a SPAN (port mirroring) port on the core switch.

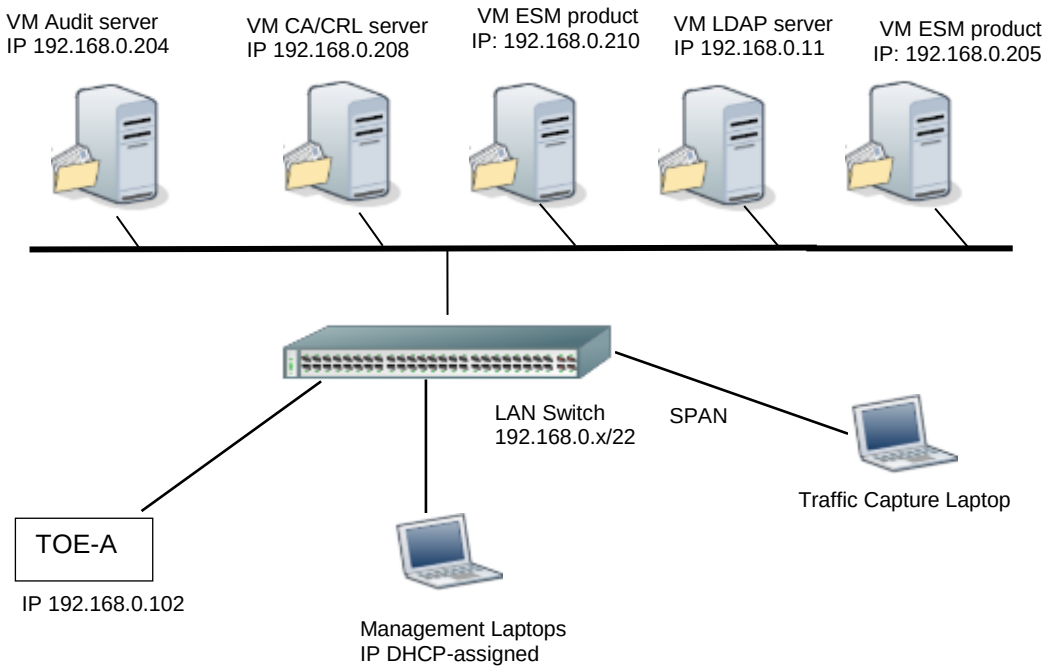

Figure 1: Network Topology

2 Security Functional Requirements

2.1 Enterprise Security Management (ESM)

2.1.1 *ESM_EAU.2 Reliance on Enterprise Authentication*

2.1.1.1 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.

2.1.1.2 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 CC GUIDE, 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 CC GUIDE. 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 CC GUIDE, 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.

2.1.1.3 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) In the TR PP-2 Test 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) In the TR PP-2 Test 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.

2.1.2 *ESM_EID.1 Reliance on Enterprise Identification*

2.1.2.1 Assurance Activities

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

2.1.3 *ESM_ICD.1 Identity and Credential Definition*

2.1.3.1 TSS Assurance Activities

TSS Assurance Activities: *(1) The evaluator shall review the TSS to verify that it identifies compatible ESM products and …* *(2) … describes the identity and credential data that are used by those products.* *(3) 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: The ST, Section 1.3.2, 'TOE Usage' defines the TOE: "*The TOE is an enterprise application designed to store, distribute, change, and audit use of enterprise user credentials in a secure environment*". This definition is further expanded in the ST Section 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…with the TOE providing the credentials on behalf of the Enterprise User*". In this context the evaluator understands "compatible ESM products" as managed systems and identity and credential data as internal objects, or Secrets. (1) The ST, Section 7.1.2, identifies the compatible ESM product as IT assets compatible with specific credential types: Windows Account, Active Directory Account, Unix Account (SSH). The TSS also offers an example – Unix Account (SSH) used to manage a CentOS server. The evaluator understands this as describing compatible ESM product based on interoperability, with this definition approximately corresponding to any modern Linux system based on Kernel 2.6.32 and later, any Windows Server 2008 R2 or later, any Windows 7 Enterprise or later systems. The evaluator concludes that such a description would be clear to a typical TOE user (sysadmin) and determines that creating exhaustive list of compatible system to be impractical and unnecessary. Therefore, the TSS adequately identifies compatible ESM products. (2) The ST, Section 7.1.2, explains that the TOE extends the identity of enrolled enterprise users and describes these extensions in terms of internal objects that contain identity and credential data

used to access managed enterprise IT assets. The TSS explains that there are two types of internal objects: Secrets and Secret Templates. The ST Table 13 describes the internal structure of these objects. The ST Section 7.1.3 describes the transmission of the identity and credential data that is used by managed IT assets. The overall picture that the TSS presents can be understood as follows: Users authenticate to the TOE using domain credentials, and then, based on Secrets that contain specific managed credentials, access TOE-managed IT assets in the enterprise environment. The list of supported credential types (Unix Account (SSH), Active Directory Account, Windows Account) provides the evaluator with sufficient information to understand the identity and credential data used by those products.

(3) The evaluator reviewed public documentation for the SSH Unix Account and the Putty Launcher (https://www.ssh.com/ssh/putty/putty-manuals/0.68/index.html), and verified that Putty is an SSH-based tool that can be used to remotely access a Unix/Linux-based system securely through an untrusted network. Putty supports several authentication methods, including using the username + password set of credentials.

The evaluator then reviewed public documentation for Microsoft Active Directory and Windows Accounts and RDP Launcher, and verified that each of these can also use username + password authentication data in a compatible way as asserted by the TSS. The evaluator then confirmed with the public documentation for the RDP Launcher (https://security.berkeley.edu/resources/best-practices-how-articles/system-application-security/securing-remote-desktop-rdp-system) that the RDP Launcher can work in conjunction with Active Directory and specific username + password credentials to access a Windows platform.

Following from these investigations, the evaluator confirmed that both the RDP Launcher used for remote Windows desktop sessions, and the Putty Launcher used for Unix/Linux CLI access over SSH, can operate over a secure channel with the username + password set of credentials. The evaluator concluded that this is compatible with the expectations outlined in the PP and is consistent with the description provided in the TSS Section 7.1.2.

2.1.3.2 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 CC GUIDE, Section 5.2 and 7.1 mentions that the TOE, 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 CC GUIDE Section 9.1 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: ! @ # $ % ^ & * ( )

The CC GUIDE Section 10.1 discusses creation of Secrets. The CC GUIDE Section 10.3, Configuring Password Policy For Secret Templates, describes recommended policy for auto-generated password in Secrets.

(b) The CC GUIDE, Section 10.4 states that Secret Server uses RSA keys of 2048 bits or higher for secure authentication. These SSH keys are non-password credentials that can be managed by Secret Server.

2.1.3.3 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) In the TR [PP-1A,PP-1B, PP-3] :The evaluator created multiple secrets based on “Active Directory Account” and “Unix Account (SSH)” Templates, and then used:

- The Putty Launcher tool with a Unix Account (SSH) Secret to get CLI access to a Unix/Linux compatible system.
- The RDP Launcher tool with a Windows Account and Active Directory Account Secret to get a remote desktop session to a Windows-based machine.

Putty (https://en.wikipedia.org/wiki/PuTTY), on which Putty Launcher is based, is an open-source terminal emulator GUI tool that supports secure connections to remote hosts. One of the documented Putty features is support for secure remote terminal session over the SSH protocol. In this mode of operation Putty establishes an encrypted session to a remote system and electronically transmits encrypted username and either a password or a private key. These credentials are managed and supplied by the TOE and are part of Secret.

The ST claims to support Linux 2.6.32 or later ESM products, represented by CentOS 7 in the test setup. The evaluator methodically reviewed the published specifications for Linux (https://en.wikipedia.org/wiki/Linux) and determined that it is offered with out of the box support for SSH (https://www.ssh.com/ssh/). The evaluator further examined these specifications to confirm that Linux supports user authentication options that include a username and password or public key. During testing the evaluator confirmed that selected managed system, CentOS 7, operates consistently with this documentation. Therefore, it was concluded that CentOS 7 is representative of "Linux 2.6.32 or later" and that no further testing to confirm support for SSH and user name and password or public key authentication is necessary.

Remote Desktop Launcher (RDP) supports opening a secure RDP session (https://en.wikipedia.org/wiki/Remote_Desktop_Protocol) with a remote Windows host. One of the documented RDP features is support for secure remote graphic remoting over the RDP protocol (https://msdn.microsoft.com/en-us/library/cc240445.aspx) that is secured with TLS. In this mode of operation RDP establishes an encrypted TLS session to a remote Windows-based system and electronically transmits encrypted username and either a password or a private key. These credentials are managed and supplied by the TOE and are part of Secret.

The ST claims to support, Windows Server 2008 R2 or later, Windows 7 Enterprise or later ESM products, represented by Windows 7 Enterprise in the test setup. The evaluator methodically reviewed the published specification for Windows (https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-supported-config) and determine that it is offered with out of the box support for RDP. The evaluator further examined these specifications to confirm that Windows supports user authentication options that include a username and password or public key. During testing the evaluator confirmed that the selected managed system, Windows 7, operates consistently with this documentation. Therefore, it was concluded that Windows 7 is representative of the claimed systems and that no further testing to confirm support for RDP and user name and password or public key authentication is necessary.

Based on observing successful remote sessions, the evaluator concluded that the TOE transmitted appropriate credentials to the compatible ESM products for consumption.

The evaluator also utilized the automatic password change feature, observing a successful password change as confirmed by a subsequently rejected manual attempt to use the old password, and concluded that the TOE does create identity and credential data for consumption by the compatible ESM products.

(2) In the TR [PP-4A - PP-4F]: For the creation of a secret, the evaluator both auto-generated a password and entered one manually to test the password complexity rules.

- The evaluator tested the enforcement of password complexity rules for manual entry of secrets, by attempting to enter passwords of various composition to confirm the password complexity requirements are enforced.
- For the auto-generated secrets, the 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 a new password was generated.

(3) In the TR PP-4G: For password-based credentials, the evaluator tested policy enforcement for auto-generated and manually-generated passwords as follows: character set, minimum length, password composition – special characters, password composition – numbers, password reuse, and confirmed that the TOE correctly enforces any configured password policy for either the local users or for the secrets

(4) In the TR PP-5: For non-password based credentials: The evaluator utilized the TSF to generate an RSA key of 2048 bits size and then used the newly-generated RSA key in an SSH account secret type.

2.1.4 *ESM_ICT.1 Identity and Credential Transmission*

2.1.4.1 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 6.1.1.4 contains:

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]] with assignment corresponding to *"[when requested by an authorized TOE user]*".

The ESM ICM Protection Profile, Section 5.1.5.1 application note states:

"The intent of this requirement is to ensure that the TSF is making the identity and credential data it defines available to the Operational Environment in a timely manner so that there is assurance that the correct data is being used in the enforcement of various policies."

As per page 63 of the ESM ICM PP, there is only one assignment in the SFR ESM_ICT.1.1, which is explicitly written as **[assignment: other circumstances]**. The wording in the assignment section of this same SFR in section 6.1.1.4 is [when requested by an authorized TOE user]. This is appropriate wording for this portion of the SFR, as it clearly describes the additional circumstances for the identity and credential data to be transmitted from the TOE to compatible and authorized ESM products. Thus the assignment statement has been filled out correctly in the ST.

In the TSS portion of the ST, Section 7.1.3 states that the TOE implements a remote password change functionality that enables administrators to initiate an immediate, scheduled, or periodic password rotation. The TSS proceeds to explain that each update takes effect following the transmission of the modified credential data by the TOE to the managed IT asset, that credential data (part of an internal object called Secret) consists of user name, password, and optionally non-password credentials such as RSA keys, and that modified credential data takes effect immediately following the transmission. Based on this description, the evaluator determined that the mentioned TOE behavior is consistent with the intent mentioned in the application note. It is assumed that an administrator will act in a timely manner to initiate password change, and it is also assumed that the organization's security policy will have the TOE administrators appropriately set the periodic automatic password rotation, and that the ESM product is not offline.

(2) In the TSS portion of the ST, Section 7.1.3 states that the TOE implements remote password change functionality that enables administrators to trigger a one-time change or schedule periodic automatic password rotation of managed platforms. The TSS lists the types of Secrets (Unix Account (SSH), Windows Account, and an Active Directory Account) and protocols used (SSHv2, RDP over TLS). From this description it is clear what data is transmitted for each type of Secret being transmitted to other ESM products. The evaluator understands the circumstances to be adequately explained by an immediate, scheduled, or periodic expiring and replacement of passwords contained in Secrets.

The ST, Section 7.1.3, also states that the TOE supports the Secure LDAP (LDAPS) protocol for communication with a compatible authentication server (Active Directory). The TSS then proceeds to explain the LDAP protocol and describe the types of data that the TSF transmits and how that data maps to Secrets. The TSS also states that synchronization with Active Directory is periodic, with an administrator-configurable polling period.

2.1.4.2 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:
CC GUIDE, Section 10.0, Managing Secrets, describes how to create and update identity and credential data. CC GUIDE, Section 10.5.5 describes how to enable remote password changing, Section 10.5.6 describers configuring key rotation, and Section 10.6.5 describes automatic changing of expired secrets.. These sections include numerous screenshots that describe interactive Web-based interface that is straightforward and understandable. Base on step-by-step instructions, that are appropriate and expected presentation format for a guidance document, it is possible to understand under which circumstances new or updated data (Secrets) are transmitted to consuming ESM products.

2.1.4.3 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) In the TR PP-6A: The evaluator configured an automatic password change (part of the Secret) and observed secure transmission of existing username and password followed by commands that changed the password of managed system. Evaluator used the old username and password and confirmed it no longer works with the managed system. In the TR PP-4A, PP-5, PP-6A and PP-6B, the evaluator used Unix Account (SSH) Secret to access CentOS 7 based system using Putty launcher and Windows Account and Active Directory Account Secrets to access Windows 7 system using RDP Launcher. The evaluator examined traffic exchange and confirmed credentials are not sent in the clear.

(2) In the TR PP-6B: 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. In either the use of the RDP or the Putty launchers, the evaluator had to enter a username, a password and an IP address to be able to access the managed assets.

(3) In the TR PP-6C: As part of the test case PP-6C: Delete domain account, observe periodic synchronization, confirm old domain credentials no longer work and concluded it was removed as active data. There is no way to attempt to use deleted Secret, as it is removed from the list of available Secrets.

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 [CC GUIDE] 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 [CC GUIDE] 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_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
FTA_TSE.1	Denial of session establishment	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 Activities	CC Guide
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Section 5.0
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Section 6.0, 7.0
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	Section 10.0
	Management of credential status	Section 10.6
	Enrollment of users into repository	Section 6.0, 7.0
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed	Section 7.1.1, 10.5
FAU_STG_EXT.1	Configuration of external audit storage location	Section 11.3.2, 12.0
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	Section 5.3
	Management of actions to be taken in the event of an authentication failure	Section 5.3
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	Section 8.0
FMT_MOF.1	Management of sets of users that can interact with security functions	Section 8.0
FMT_SMR.1	Management of the users that belong to a particular role	Section 6.0, 7.0
FTA_SSL.3	Configuration of the inactivity period for session termination	Section 5.5
FTA_TAB.1	Maintenance of the banner	Section 5.4
FTA_TSE.1	Management of session establishment conditions	Section 5.6
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	Section 11.3, 13.0
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	Section 3.0, 5.0

As related to Security Audit, CC GUIDE 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 CC GUIDE 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:

In the TR PP-7: The TOE uses the Windows Event Log for local audit and an external syslog server for external audit. The ST Table 14 defines the mandatory auditable events in context of this evaluation. Generation of these audit events was tested as part of a dedicated test case, and confirmed as being generated as expected during all other testing activities. During examination of the Syslog repository, the evaluator confirmed that the audit events recorded in the repository were identical to the audit records that were written by the TOE to its local audit trail. Combined, these activities allowed the evaluator to gain confidence that the TOE's audit capability is functioning correctly.

In the TR PP-7: The evaluator noted that specific protocol failure audit events were generated by the host platform and not the TOE. In discussions with the vendor it was determined that the TOE has no visibility into such events and could not audit such events independently. Since the TOE fully relies on host platform functionality to implement all protocol functionality, the evaluator considers this acceptable. Additionally, the evaluator submitted TRRT Technical Query 569 regarding acceptability of such implementation, that resulted in an agreement with (and confirmation of) the evaluator's decision.

See the table below for detailed mapping of test cases to audit functionality:

Component	Auditable Events	Test Case
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-1A, PP-1B, PP-3, PP-4A, PP-4B, PP-4C, PP-4D, PP-4E, PP-4F, PP-4G.
	Enrollment or modification of subject	PP-11A
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
FTA_TSE.1	Denial of session establishment	PP-17
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) In the TR PP-8: T*he 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) In the TR PP-8: *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

The ST, Section 7.3 also states that the TOE relies on the operational environment to implement protocol functionality. It follows that implementation of all optional characteristics is OE functionality. In general terms, the evaluator understood that this OE functionality includes TLS v1.1 or TLS v1.2 with certificate-based server authentication, with a known set of ciphersuites to be used for LDAPS and syslog over TLS.

(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 Microsoft Windows Server 2016

Secure Channel (schannel). All cryptographic primitives, including encryption and decryption, are implemented by the operational environment.

c. The evaluator verified The CC GUIDE 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 CC GUIDE, 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) In the TR PP-[9A to 9C]: 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 and 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 CC GUIDE, 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: *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: 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 from the TOE (i.e. generated secrets) or by way of membership in groups and/or roles (the TOE associates secrets with the user's memberships within an LDAP directory such as Active Directory). 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 first 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 user's current logged-in session as maintained by the TOE. The ST, Section 7.4 states that attribute changes for a user via the TOE are immediate, and therefore take effect during the user's 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 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 CC GUIDE Section 6 and 7, which state that users accounts logging into the TOE can be local users or domain users. Local users are authenticated locally using the TOE's database, however users who authenticate using their Active Directory credentials are authenticated through the AD server. A TOE administrator uses the TOE's WebUI to add an external authentication server: in this instance the AD server. The TOE communicates to the AD server using LDAP over TLS, which is a secured channel. During its first synchronization with the AD server, the TOE imports just the usernames of the AD security group members to its local database. The TOE administrator maps this external domain group to a configured group role. Every time a domain user tries to login to the TOE WebUI, the TOE will take the domain user credential, send it to the AD server through a secure channel and wait for the active directory server to reply with a successfully authentication message, which allows the TOE to grant the user login access, or deny the user access if the TOE receives an "authentication failed" message from the AD server. The CC GUIDE Section 7.2.1, states that if the AD user account has been updated or removed, these changes will be reflected immediately in the TOE. If the connection between Secret Server and the AD domain breaks, domain users will fail to authenticate into Secret Server until the connection is re-established. Secret Server will log all failed authentication attempts by users.

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 7.5.4 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 7.5.4 states that the TOE and the SQL database are installed on the same hardware and OS. Communications with the SQL database is secured in the following way: “operating system enforces database access permissions and prevents unauthorized access”

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 CC GUIDE. Section 8.0 lists the following roles: • Administrator • User • Read Only User Table 5 of Section 8.2 details, at a basic level, which management functions can be performed by which roles. • Read Only User can list and search through all of the Secrets. • User can request access to a Secret, then use it to launch a session on a managed IT asset. • Administrator can create and manage: Secrets, groups, roles, containers, Secret policy, local accounts. Administrator can configure: the TOE’s security functionality, IIS, SQL, syslog. Table 6 of Section 8.3 provides greater granularity or detail on the TOE’s Common Criteria management activities, in which only the Administrator role can: • Define and manage identity and credential data, subject security attributes • manage credential status • configure the external audit storage location • enroll users into the TOE’s repository • manage authentication failure threshold and actions to take if authentication fails • Configure actions requiring trusted channels and paths (if applicable) • Manage user membership in roles, users that can interact with security functions • Configure inactivity timeout

- Maintain the TOE's login banner

Between them, Tables 5 and 6 make it clear that a Read Only User can view but not use Secrets, a User can use their assigned Secret(s) to access TOE-managed IT assets, and the Administrator performs all actual management of data managed by the TOE.

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) As part of Test Case PP-12, the evaluator created multiple new users and assigned these users to each claimed user role (i.e. Read-only, User, Administrator). The evaluator used each of those users to log-in into the TOE and verify access permissions. The evaluator confirmed that each role had a different set of permissions, and that only the Administrator role had access to management functions as claimed in the SFR FMT_SMF.1 as indicated by ability to access administrator-specific menu options in the UI. The administrative accounts were used throughout most of the remaining test cases. The testing of individual management activities was accomplished throughout the testing activities, see table below for details:

Requirement	Management Activities	Test Case
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	PP-1A, PP-4B, PP-4D, PP-4G
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	PP-1A, PP-4B, PP-4D, PP-4G, PP-11A, PP-11B
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	PP-3, PP-4F, PP-4E
	Management of credential status	PP-4A, PP-4C, PP-4G, PP-4F
	Enrollment of users into repository	PP-4D, PP-4B
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed	Pp-5, PP-6A, PP-6B, PP-6C
FAU_STG_EXT.1	Configuration of external audit storage location	PP-8, PP-7
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	PP-10
	Management of actions to be taken in the event of an authentication failure	PP-10
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	PP-11A, PP-11B
FMT_MOF.1	Management of sets of users that can interact with	PP-11B, PP-12

	security functions	
FMT_SMR.1	Management of the users that belong to a particular role	PP-11A, PP-11B, PP-12
FTA_SSL.3	Configuration of the inactivity period for session termination	PP-14
FTA_TAB.1	Maintenance of the banner	PP-13
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	PP-18A, PP-18B
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	PP-19

(2) As part of Test Case PP-12, the evaluator created and assigned multiple users to each claimed user role (Read-only, User). The evaluator used each of those accounts to log-in into the TOE. While logged in, the evaluator confirmed that each role had a different set of permissions, and that they could not see or access the "ADMIN" menu in the UI, through which, all the management activities are accessed. Therefore the evaluator concluded that any user with a role of "User" or "Read-only" does not have access to management functions and is disallowed from performing them.

(3) As part of Test Case PP-18A, the evaluator established a connection with an Active Directory (AD) server in the operational environment, collecting packet data during the session. Based on this packet capture, the evaluator confirmed that the TOE established a TLS-based secure channel that was authenticated with a X.509v3 server certificate. When the evaluator substituted the AD's server certificate with an untrusted certificate, the TOE rejected the connection attempt. Based on this, the evaluator concluded that the interface between these two components is secure.

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) In the ESM ICM PP, the two assignment statements for FMT_MOF.1 are [*list of functions*] and [*the authorized roles*]. In section 6.1.5.1, these assignments are [*specified in Table 15*] and [*the specified roles*].

The row entries in Table 15 in section 6.1.5.1 of the ST collectively imply that all management functions for the TOE are in fact restricted to the Administrator role.

The first sentence in section 7.5.1 of the TSS section of the ST then states directly: the TOE only permits authorized administrators to perform management functions. There is no ambiguity in this statement. The PP left the definition wide open, the SFR narrowed it, and the TSS made it very clear: only authorized administrators can perform manage functions for the TOE, as per the assignment statements.

(2) The first sentence of section 7.5.1 of the TSS states that only authorized administrators can perform management functions on the TOE. The remainder of that paragraph goes into greater detail on the authentication process for the credentials provided by the administrator. Once an administrator's credentials are authenticated, that administrator then has full management control over 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 CC GUIDE, Section 8, describes how the TOE restricts access to management functions based on roles. This includes assigning roles to users, and identifying which roles are permitted to perform specific management functions (including the management of attributes). These roles, and their permitted management functions, are shown in the table below.

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
Administrator	Create, manage, and unlock local accounts
Administrator	Configure remote audit server

The CC GUIDE, Section 8, also describes which roles are permitted to perform specific management functions that are identified specifically for Common Criteria, including the management of attributes. These roles, and their permitted management functions, are shown in the table below.

Requirement	Management Activities	Role
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 subject security attributes	Administrator
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
FTA_TSE.1	Management of session establishment conditions	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:

1) 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.

2) 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.

3) *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:

1) The management functions, in the context of Common Criteria, are defined in Table 15 of the ST. Access to these management functions by specific roles was tested in both the dedicated test case PP-12 where access to management functions under the Administration tab was confirmed, and as part of the rest of the testing effort where individual management functions were exercised.

2) The TOE does not claim to be compatible with any secure configuration management product, consequently such functionality was not tested.

3) Access restrictions for which roles can access and exercise specific management functions were addressed in test cases PP-11B and PP-12, where a subset of management functions were tested. It was also determined that unprivileged accounts are unable to access management functions.

   Combined, these activities allowed the evaluators to determine that the TOE's administrative accounts have appropriate permissions, that the non-administrative roles do not have access to management functions, and that there is no obvious way to bypass the TOE's access control restrictions or to escalate user privileges.

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

2.5.3.2 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 CC GUIDE, Section 8.2 Management Functions based on role, defines all of the management functions and the corresponding user roles. The CC GUIDE document describes how to perform those management functions and the outcome of every function perfumed by each role. The below table lists the management functions and the corresponding CC GUIDE sections that details it.

Requirement	Management Activities	CC Guide
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Section 5.0
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Section 6.0, 7.0
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	Section 10.0
	Management of credential status	Section 10.6
	Enrollment of users into repository	Section 6.0, 7.0
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed	Section 7.1.1, 10.4
FAU_STG_EXT.1	Configuration of external audit storage location	Section 11.3.2, 12.0
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	Section 5.3
	Management of actions to be taken in the event of an authentication failure	Section 5.3
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	Section 8.0
FMT_MOF.1	Management of sets of users that can interact with security functions	Section 8.0
FMT_SMR.1	Management of the users that belong to a particular role	Section 6.0, 7.0
FTA_SSL.3	Configuration of the inactivity period for session termination	Section 5.5
FTA_TAB.1	Maintenance of the banner	Section 5.4

FTA_TSE.1	Management of session establishment conditions	Section 5.6
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	Section 11.3, 13.0
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	Section 3.0, 5.0

2.5.3.3 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:
As part of the PP-12 Test Case, the evaluator verified that management functions exist and are accessible only by users with appropriate roles (i.e. administrators). The TOE implements a Web-based management interface, as such access (or lack of thereof) to management functions is clear based on the interface options presented to a logged-in user. Throughout the rest of the testing effort, individual management functions defined in the ST were exercised (see below mapping table) and the evaluator determined that they work in the prescribed manner. Since each management function listed in FMT_SMF.1 is tied to security functionality defined in other SFRs, and since all testing assurance activities for these SFRs were carried out, the evaluator concluded that this assurance activity is therefore satisfied.

Requirement	Management Functions	Test Case
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	PP-1A, PP-4B, PP-4D, PP-4G
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	PP-1A, PP-4B, PP-4D, PP-4G, PP-11A, PP-11B
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	PP-3, PP-4F, PP-4E
	Management of credential status	PP-4A, PP-4C, PP-4G, PP-4F
	Enrollment of users into repository	PP-4D, PP-4B
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed	Pp-5, PP-6A, PP-6B, PP-6C
FAU_STG_EXT.1	Configuration of external audit storage location	PP-8, PP-7
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts	PP-10
	Management of actions to be taken in the event of an authentication failure	PP-10
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	PP-11A, PP-11B
FMT_MOF.1	Management of sets of users that can interact with security functions	PP-11B, PP-12
FMT_SMR.1	Management of the users that belong to a particular	PP-11A, PP-11B, PP-12

	role	
FTA_SSL.3	Configuration of the inactivity period for session termination	PP-14
FTA_TAB.1	Maintenance of the banner	PP-13
FTA_TSE.1	Management of session establishment conditions	PP-17
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	PP-18A, PP-18B
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	PP-19

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 Table 15 in the ST document.

(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 CC GUIDE, Section 8.0 Common Criteria Roles and Permissions, describes Administrator, User, Read Only User as roles that “comply with Common Criteria standards”. The CC GUIDE, Section 8.1 Assigning Roles to Users, describes how to assign users to roles.

2.5.4.3 Testing Assurance Activities

Testing Assurance Activities:

1) 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.

2) *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:

1) In the TR PP 11A-B and PP-12: 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. 2) In TR PP-11C: as 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) The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be vifwed 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 7.6.1 details that local authentication data and Secrets are protected by the Operating Environment, which, in turn, utilizes encryption to obscure the plaintext credential data. The evaluator determined that this covers all of the authentication data (other than private keys) used by the TOE. (2) The ST, Sections 7.6.1 Section 7.6.2, explain that user credentials are stored as encrypted data in the database, and that the Operating Environment implements these protections via Access Control Lists (ACLs) and the Microsoft Data Protection API (DPAPI). Based on the publically-available information on Microsoft ACLs and the Microsoft DPAPI, the evaluator has concluded that these Operating Environment features constitute adequate protections for all authentication data.

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:
1) *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.* 2) *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: 1) 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. 2) In TR PP-15A-B: 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 2016 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 2016 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 CC GUIDE, 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 CC GUIDE, 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 CC GUIDE, 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: In TR PP-16: 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 CC GUIDE, 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: In the TR PP-17: 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 CC GUIDE, Section 7.1.3 and noted it describes how to configure TLS for Active Directory. The CC GUIDE, 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 CC 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 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 CC GUIDE, 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:
(1) *The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE.* (2) *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:
(1) Microsoft Windows Server 2016 comes with a FIPS-validated cryptographic module (the CryptoAPI) as part of the core operating system. This is expected functionality that is effectively built into the operating system. Applications built to run on Windows Server 2016 (such as the TOE), that are designed to rely on cryptographic services in their operating environment, will be able to utilize this built-in cryptographic module via the publically-available CryptoAPI interfaces, when it is needed. The CC GUIDE contains instructions on enabling Microsoft FIPS Module support and choosing the clamed ciphersuites are performed during the Installation of the TOE. (2) The CC GUIDE, section 11.1.4, does provide the warning “The use of other cryptographic engines was not evaluated nor supported in the Common Criteria configuration.”

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 ST section 1.4.2.1 Physical boundary identifies the TOE as a software application. The TOE software is delivered as an MSI installer package (ThycoticSetup.exe as per the CC Guide section 2.3.1) that is compatible with windows installer 5.0 that deploys an ASP.NET application. The ST v2.0 Section 1.4.1.1 Table 2 specifies Microsoft Windows Server 2016 (x64) as a minimum requirement. Windows Server 2016 ships with .NET 4.6.2 included as a core component of the OS; .NET 4.6.2 is backwards compatible with all previous 4.x versions. The latest version, .NET 4.7.2, is also fully backwards compatible. The ST Sections 1.2 and 1.4.1.1 identify the TOE's minimum hardware requirements for a CPU as an Intel Core i5, which is a 2.4 GHz 4-core 64-bit Intel processor. This matches Section 2.1 of the CC Guide, which also calls for an Intel Core i5 as a minimum). All of the CPUs claimed in the ST Section 1.2 implement the x86-64 instruction set. Additionally, Intel shares the same processor microarchitecture across multiple product lines – the Xeon E5, Core i5, and Core i7. As such, the differences between these CPUs are limited to: the number of cores, core speed, FSB speed, the number and type of host adapters, and so on. In simple terms, this means that how fast data is shuffled, how much of it is accessed at the same time, and how the scheduler prioritizes individual instructions may vary, but how the code path is executed does *not* vary.

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 10.1, 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 CC GUIDE guide, and they both identify the TOE as Thycotic Secret Server Government Edition, Version 10.1, 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 v0.9 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 requested that the vendor provide a comprehensive list of third-party components used by the TOE. Using this list, the evaluator identified 165 libraries, toolkits, and components. The evaluator then performed searches on public information from the following sources: • National Vulnerability Database (https://nvd.nist.gov) • CVE details (https://www.cvedetails.com) • Open Sourced Vulnerability Database (vulners.com) • Security Focus (securityfocus.com) Using search terms that included: “Thycotic”, “Secret Server”, “.NET”. These searches produced a combined list of 26 potential vulnerabilities. The evaluator then reviewed this list based on criteria including: applicability to each component (version affected), whether or not the vulnerable functionality might be utilized by the TOE, etc. A much shorter list of potential vulnerabilities was forwarded to the vendor, who performed a thorough granular search on whether or not the TOE used specific functionality (i.e. a function call), and either upgraded the component in question or provided a rationale back to the evaluator that either required further clarification or was determined to be appropriate as to why the vulnerability did not apply.

4 Appendix: Results of ST and TOE Evaluation

4.1.1 *Results of the ST evaluation*

The overall results of the ST evaluation are summarized in the table below as verdicts for each evaluator activity.

Table 3: Summary of Results of ST Evaluation

Component	Element	Work Unit	Verdict
ASE_INT.1			**Pass**
	ASE_INT.1.1E		
		ASE_INT.1-1	Pass
		ASE_INT.1-2	Pass
		ASE_INT.1-3	Pass
		ASE_INT.1-4	Pass
		ASE_INT.1-5	Pass

Component	Element	Work Unit	Verdict
		ASE_INT.1-6	Pass
		ASE_INT.1-7	Pass
		ASE_INT.1-8	Pass
		ASE_INT.1-9	Pass
		ASE_INT.1-10	Pass
	ASE_INT.1.1E		
		ASE_INT.1-11	Pass
ASE_CCL.1			**Pass**
	ASE_CCL.1.1E		
		ASE_CCL.1-1	Pass
		ASE_CCL.1-2	Pass
		ASE_CCL.1-3	Pass
		ASE_CCL.1-4	Pass
		ASE_CCL.1-5	Pass
		ASE_CCL.1-6	Pass
		ASE_CCL.1-7	Pass
		ASE_CCL.1-8	Pass
		ASE_CCL.1-9	Pass
		ASE_CCL.1-10	Pass
		ASE_CCL.1-11	Pass
		ASE_CCL.1-12	Pass
ASE_OBJ.1			**Pass**
	ASE_OBJ.1.1E		
		ASE_OBJ.1-1	Pass
ASE_ECD.1			**Pass**
	ASE_ECD.1.1E		
		ASE_ECD.1-1	Pass
		ASE_ECD.1-2	Pass
		ASE_ECD.1-3	Pass
		ASE_ECD.1-4	Pass
		ASE_ECD.1-5	Pass
		ASE_ECD.1-6	Pass
		ASE_ECD.1-7	Pass
		ASE_ECD.1-8	Pass
		ASE_ECD.1-9	Pass
		ASE_ECD.1-10	Pass
		ASE_ECD.1-11	Pass
		ASE_ECD.1-12	Pass
	ASE_ECD.1.2E		
		ASE_ECD.1-13	Pass
ASE_REQ.1			**Pass**
	ASE_REQ.1.1E		

Component	Element	Work Unit	Verdict
		ASE_REQ.1-1	Pass
		ASE_REQ.1-2	Pass
		ASE_REQ.1-3	Pass
		ASE_REQ.1-4	Pass
		ASE_REQ.1-5	Pass
		ASE_REQ.1-6	Pass
		ASE_REQ.1-7	Pass
		ASE_REQ.1-8	Pass
		ASE_REQ.1-9	Pass
		ASE_REQ.1-10	Pass
ASE_TSS.1			**Pass**
	ASE_TSS.1.1E		
		ASE_TSS.1-1	Pass
	ASE_TSS.1.2E		
		ASE_TSS.1-2	Pass

4.1.2 *Results of the TOE evaluation*

The overall results of the TOE evaluation are summarized in the following table as verdicts for each evaluator activity and EAL 1 TOE assurance component.

Table 4: Summary of Results of TOE Evaluation

Class	Component	Action Element	Verdict
ADV			**Pass**
	ADV_FSP.1		Pass
		ADV_FSP.1.1E	Pass
		ADV_FSP.1.2E	Pass
AGD			**Pass**
	AGD_OPE.1		Pass
		AGD_OPE.1.1E	Pass
	AGD_PRE.1		Pass
		AGD_PRE.1.1E	Pass
		AGD_PRE.1.2E	Pass
ALC			**Pass**
	ALC_CMC.1		Pass

Class	Component	Action Element	Verdict
		ALC_CMC.1.1E	Pass
	ALC_CMS.1		Pass
		ALC_CMS.1.1E	Pass
ATE			**Pass**
	ATE_IND.1		Pass
		ATE_IND.1.1E	Pass
		ATE_IND.1.2E	Pass
AVA			**Pass**
	AVA_VAN.1		Pass
		AVA_VAN.1.1E	Pass
		AVA_VAN.1.2E	Pass
		AVA_VAN.1.3E	Pass