20 SEPTEMBER 2020

Document Version 1.0

CYSECA

CYSECA ENDPOINT APPLICATION CONTROL SECURITY TARGET

For more information visit us at

www.cyseca.com.my

Document management

Document identification

Document ID	CYSECA_EAL2_ST
Document title	CYSECA Endpoint Application Control Security Target
Prepared by	Muzamir Mohamad
Release Authority	Pernec Integrated Network Systems Sdn. Bhd.
Document Version/Date	Version 1.0, 20-SEPT-2020

Document history

Version	Date	Description
0.1	08-OCT-19	Released for internal review (ST Lite)
0.2	20- NOV-19	Update the version of client (ST Lite)
0.3	07-FEB-20	Add TOE Summary Specification
0.4	09-MAR-20	Update the newer Server v1.0.0
0.5	05-MAY-20	Update Section 1.4.1, 1.5.1, 2.0, 6.2.12, 6.3.1,8.2, 8.4 and 8.6.
0.6	19-JUN-20	Update Section 1.4.1 and 6.3.2
1.0	20-SEPT-20	Final Released

Table of Contents

1 Security Target Introduction (ASE_INT.1)

1.1 ST Reference

ST Title	CYSECA Endpoint Application Control Security Target
ST Identifier	CYSECA_EAL2_ST
ST Version/Date	Version 1.0, 20-SEPT-2020

1.2 TOE Reference

TOE Title	CYSECA Endpoint Application Control which consists of: • CYSECA Endpoint Application Control Server v1.2.0 • CYSECA Endpoint Application Control Client v1.1.12
TOE Version	CYSECA Endpoint Application Control which consists of: • CYSECA Endpoint Application Control Server v1.2.0 • CYSECA Endpoint Application Control Client v1.1.12

1.3 Document Organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the extended component definitions that met by the TOE (ASE_ECD.1)
- Section 6 contains the security functional and assurance requirements derived from the Common Criteria Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 7 contains the security assurance requirements derived from the Common Criteria, Part 3 (ASE_REQ.2).

- Section 8 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 TOE Overview

1.4.1 TOE Usage and Major Security Functions

The Target of Evaluation (TOE) is CYSECA Endpoint Application Control which consists of CYSECA Endpoint Application Control Server v1.2.0 (TOE Server) and CYSECA Endpoint Application Control Client v1.1.12 (TOE Client). The TOE is an endpoint application control allows organization to enhance the defences against executing unwanted or malicious application on critical endpoint computer. TOE comprise of server and client components that can be operated in one or more instance.

Organisations are constantly facing threats that results in data leakage, locked folders with ransom note, loss of valuable data, use of compromised clients as launching pad for malicious activities and more.

They are becoming increasingly aware that traditional anti-malware defences on clients do not provide adequate control against modern threats and targeted attacks. This is made worse with thousands of new malicious software being deployed daily.

TOE is designed with granular policy, extensive application catalogue as well as, real-time monitoring and defences, CYSECA reduces the risk of threat exposures on client. The TOE is designed for Application control implementation for client and allows only selected files or applications that are allowed/whitelisted to be executed while others are being stopped.

The TOE key features include:

- Allowing access to only authorised application
- Prevents potential damage from unwanted or unknown application
- Prevent malware execution
- Detects unauthorised application from USB, browser (driver-by-attack), malware hidden within files, network propagation.
- Enforce software license compliance
- Pre-categorized application catalogue, adaptable to customization
- Central policy Management
- List running applications and terminate process
- Block read/write on USB disk drive
- Realtime monitoring executables, dashboard, email alerts

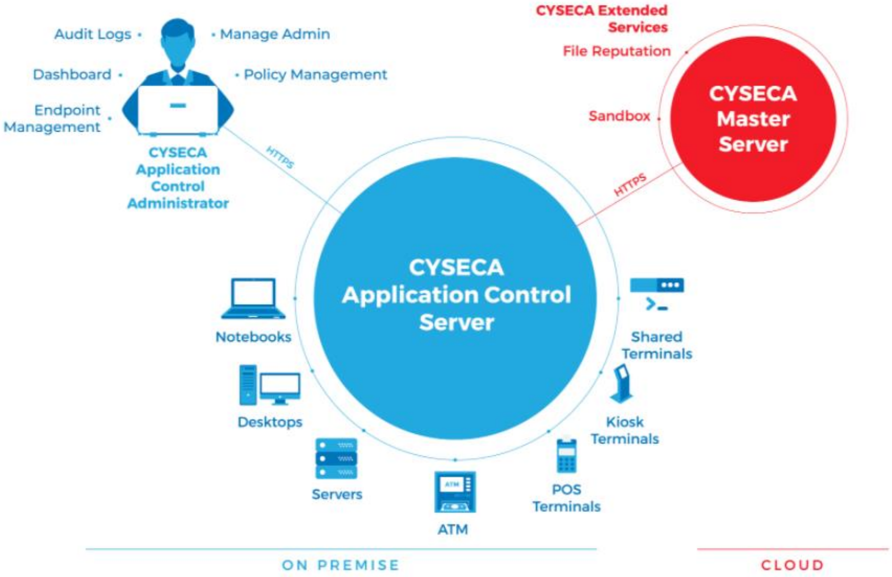

Figure 1 – TOE Overview Architecture

The following table highlights the range of security functions implemented by the TOE.

Security functions	Descriptions
Application Control (Whitelist)	The TOE is designed to prevent executing unauthorized application, unknown application, malware and zero-day malware on client. The TOE can be configured to allow authorised application to execute on client to prevent execution of unauthorized application, unknown application, malware and zero-day malware.
Audit	The TOE generates audit records for security events. Super Admin, Admin and Read-Only users have the ability to view and export the audit and transaction logs. The TOE generates audits when events, file-less and action occur, stores the audit information on the client local system, transmits the audit information to a server, generates alarms for designated events, and provides a means for audit review. Protection of audit data in the audit trail involves the TOE and the Operating System (OS). The TOE controls the insertion of audit events into the audit log and the deletion of audit events from the audit log. The OS provides basic file protection services for the audit log
Identification and Authentication	TOE users (Super Admin, Admin and Read-Only) are required to identify or authenticate with the TOE prior to any user action or information flow being permitted. TOE users may interact with the TOE via supported web browsers.
Security Management	The TOE provides Super Admin and Admin with the capabilities to configure, monitor and manage the TOE to fulfil the Security Objectives. The TOE restricts access to the management functions based on the role of the user. Security Management principles relate to Application control Rules and Audit.

Security functions	Descriptions
Secure Communication	The TOE utilizes Transport Layer Security (TLS) v1.2 cryptographic protocol to secure the communication between client web browser and the TOE.

Table 1 – Major Security Functions

1.4.2 TOE Type

The product type of the Target of Evaluation (TOE) described in this Security Target (ST) is an endpoint application control running on windows operating system computer (TOE Client), along with a management component running on server (TOE Server) to enhance the defences against executing unwanted or malicious application on critical endpoint computer. TOE provides security functionality such as Audit, Application Control (Whitelist), Identification and Authentication, Security Management and Secure Communication. The TOE can be categorised as *Other Devices and Systems* in accordance with the categories identified on the Common Criteria Portal (www.commoncriteriaportal.org) that lists all the certified products.

1.4.3 Supporting hardware, software and/or firmware

Minimum System Requirements	
TOE Client	
Operating Systems	Windows 10
Processor	Dual-Core
Memory (RAM)	1GB
Disk Storage	500 MB
Web Browser	Internet Explorer 10 Mozilla Firefox 8 Chrome 60
TOE Server	
Operating System	Ubuntu 16.04 LTS
Processor	Dual-Core
Memory (RAM)	4GB
Disk Storage	50GB

Java Runtime Environment	1.7
Java Security Policy	128-bit key restriction shall be removed to support 256-bit key
Database	MySQL Database v5.6

Table 2 – Minimum System Requirements

1.5 TOE Description

TOE is composed of CYSECA Endpoint Application Control Server v1.2.0 (called "TOE Server") and CYSECA Endpoint Application Control Client v1.1.12 (called "TOE Client"). TOE provide clients management with Application Control to prevent executing unwanted or malicious application for servers, desktops, and laptops running on Windows operating system. It provides protection against executing unwanted or malicious application. The TOE include the following components:

- TOE Client – protects servers, desktops, and laptops
- TOE Server– executes management operations

1.5.1 Physical scope of the TOE

The physical boundary of the TOE is depicted in Figure 1 (shaded in blue are within the TOE boundary).

The operating systems, web Server components and CYSECA Master Server are out of Scope of Evaluation. In order to comply with the evaluated configuration, the following hardware and software components should be used as in section 1.4.3.

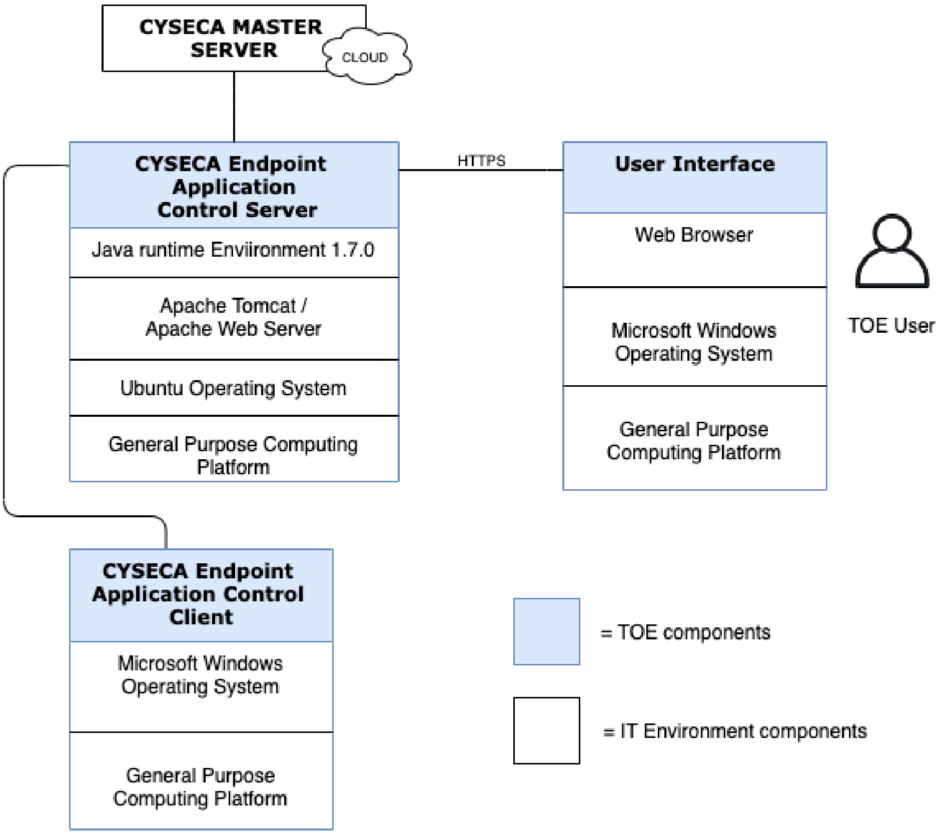
CYSECA MASTER SERVER
CLOUD
HTTPS
CYSECA Endpoint Application Control Server
Java runtime Enviironment 1.7.0
Apache Tomcat / Apache Web Server
Ubuntu Operating System
General Purpose Computing Platform
User Interface
Web Browser
Microsoft Windows Operating System
General Purpose Computing Platform
TOE User
CYSECA Endpoint Application Control Client
Microsoft Windows Operating System
General Purpose Computing Platform
= TOE components
= IT Environment components

Figure 1 – TOE Boundary

At a high level, the TOE process flow include the following:

- Software process flow for connection to internal TOE components and external IT products.
- Software process flow to receive and process traffic from internal TOE components and external IT products.
- User interface process flow to handle administrative actions.

The TOE's evaluated configuration requires one or more instances of a TOE Client, one instance of a TOE Server, and one or more instances of a workstation for management via User Interface.

PERNEC representative will install TOE Server on-premise or cloud infrastructure. The pre-configured TOE Client installer (Agent) will be distributed to endpoint client. The TOE Server's credential will shared to the TOE Super Admin.

The Physical Boundary includes the following guidance documentation:

- CYSECA User manual - Super Admin: https://awl.cyseca.com/manual/views/super-admin/super-register.html
- CYSECA User manual - Admin: https://awl.cyseca.com/manual/views/super-admin/super-register.html
- CYSECA User manual – Read Only: https://awl.cyseca.com/manual/views/read-only/read-login.html
- CYSECA User manual – Client: https://awl.cyseca.com/manual/views/client/client-install.html

1.5.2 Logical scope of the TOE

The logical boundary consists of the security functionality of TOE is summarized below.

- **Application Control (Whitelist).** The TOE is designed to help prevent executing unwanted or malicious application on clients. The TOE can be configured to allow authorised application to execute on clients.
- **Audit:** The TOE generates audit records for security events. Types of audit logs are:
  - Action Logs - Date & time, username, IP Address , Event type (refer to SFR)
  - Event Logs - Date & time, MD5, Path, Computer and Packages
  - Fileless Logs – Time, Command Line, Computer

  Only Super Admin, Admin and Read-Only has the capability to review these audit records via the user interface
- **Identification and Authentication:** All users (Super Admin, Admin and Read-Only) are required to perform identification and authentication with the TOE before any information

flows are permitted. These users must be authenticated prior to performing any TOE functions by entering a username and password.

- **Security Management**: The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access them. The Super Admin and Admin have the ability to manage read-only user and configure the TOE.
- **Secure communications.** The TOE provides a secure channel between the TOE User and the TOE by utilizing Transport Layer Security (TLS v1.2) protocols.

2 Conformance Claim (ASE_CCL.1)

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017
    - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2

3 Security Problem Definition (ASE_SPD.1)

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** are any statements made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

Identifier	**Threat statement**
T. AUDIT_ COMPROMISE	A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.
T.CONFIG	An unauthorized person may read, modify, or destroy TOE configuration data.
T. MANAGEMENT	An unauthorized user modifies configuration data that they are not authorised to access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTHORISED_ACCESS	A user may gain unauthorized access to the TOE and residing data by sending impermissible information through the TOE (such as Brute Force Attacks) resulting the exploitation of protected resources.
T. SEC_COM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between distributed components of the TOE.

Table 3 – Threats

3.3 Organisational Security Policies

No organisational security policies have been defined regarding the use of the TOE

3.4 Assumptions

Identifier	Assumption statement
A.PLATFORM	The TOE relies upon a trustworthy platform and local network from which it provides administrative capabilities. The TOE relies on this platform to provide logon services via a local or network directory service, and to provide basic audit log management functions. The platform is expected to be configured specifically to provide TOE services, employing features such as a host-based firewall which limits its network role to providing TOE functionality.
A.ADMIN	One or more competent, trusted personnel who are not careless, wilfully negligent, or hostile, are assigned and authorized as the Administrator, and do so using and abiding by guidance documentation.
A.USER	Users are not wilfully negligent or hostile and use the device within compliance of a reasonable enterprise security policy.
A.TIMESTAMP	The platforms on which the TOE operate shall be able to provide reliable time stamps.
A.PHYSICAL	It is assumed that the appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.

Table 4 – Assumptions

4 Security Objectives (ASE_OBJ.2)

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. There are security objectives for the TOE to address and additional objectives that provide specific direction for the intended in environment in which the TOE is to operate.

4.2 Security Objectives for the TOE

Identifier	Objective statements
O. ACCESS	The TOE must ensure that only authorised users are able to access protected resources or functions and to explicitly deny access to specific users when appropriate
O. AUDIT_PROTECT	The TOE will provide the capability to protect audit information.
O.CONFIG	TOE shall prevent unauthorized person to access TOE functions and configuration data. Only authorized TOE users (Super Admin and Admin) shall have access to TOE management interface.
O. MANAGE	The TOE must allow Super Admin and Admin to effectively manage the TOE, while ensuring that appropriate controls are maintained over those functions.
O.USER	The TOE must ensure that all users are identified and authenticated before accessing protected resources or functions.
O.SEC_COM	The TOE must protect the confidentiality of its dialogue between distributed components.

Table 5 – Security Objective

4.3 Security Objectives for the Environment

Identifier	Objective statements
OE. PLATFORM	The TOE relies upon the trustworthy platform and hardware to provide policy enforcement as well as cryptographic services and data protection.
OE. ADMIN	The owners of the TOE must ensure that the Super Admin and Admin who manages the TOE is not hostile, competent and apply all super user guidance in a trusted manner.

Identifier	Objective statements
OE.USER	Users of the TOE are trained to securely use the system, controller and device and apply all guidance in a trusted manner.
OE. TIMESTAMP	Reliable timestamp is provided by the operational environment for the TOE.
OE. PHYSICAL	Those responsible for the TOE must ensure that the appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.
OE.TOE_ACCESS	The IT environment will provide mechanisms that control a user's logical access to the TOE.

Table 6 – Security Objective for environment

4.4 TOE Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats and OSPs.

THREATS/ ASSUMPTIONS/ OSPs OBJECTIVES	T.AUDIT_COMPROMISE	T.MANAGEMENT	T.MASQUERADE	T.UNAUTHORISED_ACCESS	T.CONFIG	T. SEC_COM	A.PLATFORM	A.ADMIN	A.USER	A.TIMESTAMP	A.PHYSICAL
O.ACCESS		✓		✓							
O.AUDIT_PROTECT	✓										
O.CONFIG					✓						
O.MANAGE		✓									
O.USER		✓		✓							
O. SEC_COM						✓					
OE.PLATFORM							✓				
OE.ADMIN								✓			
OE.TOE_ACCESS			✓								

THREATS/ ASSUMPTIONS/ OSPs **OBJECTIVES**	**T.AUDIT_COMPROMISE**	**T.MANAGEMENT**	**T.MASQUERADE**	**T.UNAUTHORISED_ACCESS**	**T.CONFIG**	**T. SEC_COM**	**A.PLATFORM**	**A.ADMIN**	**A.USER**	**A.TIMESTAMP**	**A.PHYSICAL**
OE.USER									✓		
OE. TIMESTAMP										✓	
OE. PHYSICAL											✓

Table 7 – TOE Security Objective Rationale Table

The following table demonstrates that all security objectives for the TOE trace back to the threats and OSPs in the security problem definition.

Threats/OSPs	**Objectives**	**Rationale**
T. AUDIT_COMPROMISE	O. AUDIT_PROTECT	The objective ensures that the TOE provides the capability to protect audit information.
T.CONFIG	O.CONFIG	The objective ensures that the TOE only allowed authorized person such as Super Admin and Admin to access TOE functions and configuration data.
T. MANAGEMENT	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
	O. MANAGE	This objective ensures that the TOE provides the tools necessary for the authorized system admin to manage the security-related functions and that those tools are usable only by users with appropriate authorizations.
	O. ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users and deny access to specific users when appropriate

Threats/OSPs	Objectives	Rationale
T. MASQUERADE:	OE.TOE_ACCESS	Mitigates this threat by requiring authorized users and workstation users to be identified and authenticated, a necessary step in controlling the logical access to the TOE and its resources by constraining how and when users can access the TOE. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.
T. UNAUTHORISED_ACCESS	O. ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users and deny access to specific users when appropriate
	O.USER	The objective ensures that the TOE identifies and authenticates all users before they access a protected resources or functions.
T. SEC_COM	O. SEC_COM	The objective ensures that the TOE protect the confidentiality of its communication between distributed components.

Table 8 – TOE Security Objective Rationale

4.5 Environment Security Objectives Rationale

The following table demonstrates that all security objectives for the operational environment all trace back to assumptions or OSPs in the security problem definition.

Assumptions	Objective	Rationale
A.PLATFORM	OE.PLATFORM	This objective ensures that the underlying platforms are trustworthy and hardened to protect against known vulnerabilities and security configuration issues.
A.ADMIN	OE.ADMIN	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.

Assumptions	Objective	Rationale
A.USER	OE.USER	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of operating the TOE and the security of the information it contains in a secure manner.
A.TIMESTAMP	OE.TIMESTAMP	This objective ensures that reliable timestamps are provided by the TOE.
A.PHYSICAL	OE.PHYSICAL	This objective ensures that the appliance that hosts the operating system and database are hosted in a secure operating facility with restricted physical access with non-shared hardware.

Table 9 – Environment Security Objective Rationale

5 Extended Components (ASE_ECD.1)

This section defines the extended SFRs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table identifies all extended SFRs implemented by the TOE

Name	Description
EXT_CAC_WL.1	Application Control Whitelist
EXT_CAC_RCT.1	Application Control React

Table 10 - Extended TOE Security Functional Requirements

5.1.1 Class EXT_CAC: CYSECA Application Control

Application Control functions involve enforcement of restrictions on execution of applications on the client operating system, and on modification of files on the targeted system. The EXT_CAC: CYSECA Application Control class was modelled after the CC FAU: Security Audit class.

The extended family EXT_CAC_WL: Application Control Data Collection was modelled after the CC family FAU_GEN: Security Audit Data Generation. The extended family EXT_CAC_RCT: Application Control React was modelled after the families FAU_SAA: Potential Violation Analysis and FAU_ARP: Security Alarms.

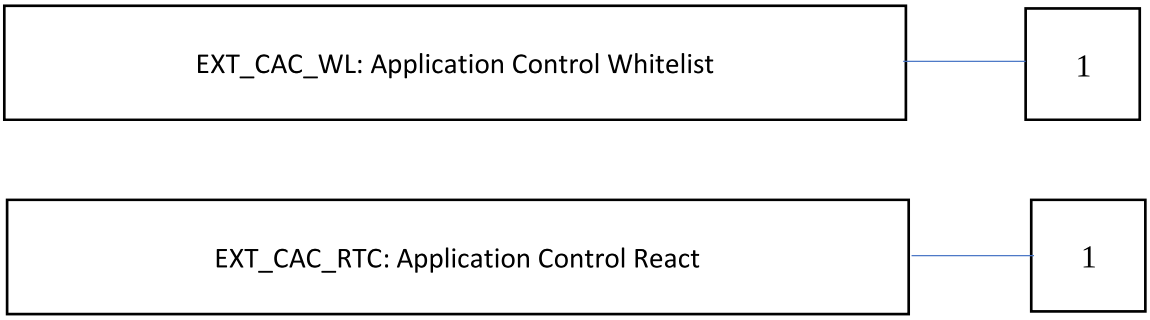
EXT_CAC_WL: Application Control Whitelist
1
EXT_CAC_RTC: Application Control React
1

Figure 2 – EXT_CAC: CYSECA Application Control Class Decomposition

5.1.1.1 CYSECA Application Control Whitelist (EXT_CAC_WL)

Family Behaviour

This family defines the requirements for creating a whitelist of application on the targeted system for use in determining which applications will be allowed to execute on the system. This family enumerates the types of program code that shall be collected by the TOE Security Function (TSF), and identifies what type of control will be enforced on the executable code.

Component Levelling

EXT_CAC_WL: Application Control Whitelist
1

Figure 3 – Application Control Data Collection family decomposition

EXT_CAC_WL.1 Application control whitelist, specifies the list of executable code that shall be allowed to run on the targeted system, as well as identifies registry keys, and executable code.

Management: EXT_CAC_WL.1

There are no management activities foreseen.

Audit: EXT_CAC_WL.1

There are no auditable events foreseen.

EXT_CAC_WL.1   Application and change control data collection

Hierarchical to: No other components

Dependencies: No dependencies

EXT_CAC_WL.1.1 The System shall be able to collect the following information from the targeted IT System resource(s): [assignment: lists of application allowed to execute].

EXT_CAC_WL.1.2 At a minimum, the System shall collect and record the following information:

- ***[assignment: list of data collected].***

5.1.1.2 CYSECA Application Control React (EXT_CAC_RCT)

Family Behaviour

This family defines the analysis the TOE performs on the collected application control data and the actions to be taken by the TOE in response to the findings of the analysis. This family enumerates the types of program code that shall be collected by the TSF, and identifies what application control will be allowed to executable code.

Component Levelling

EXT_CAC_RCT: Application Control React
1

Figure 1 – Application and Change Control

React family decomposition

EXT_CAC_RCT.1 Application control react, specifies the list of actions that shall be taken for each analytical result obtained against the collected application control data.

Management: EXT_CAC_RCT.1

- The management (allow or disallow) of actions.

Audit: EXT_CAC_RCT.1

- Minimal: Actions taken due to application analysis requirements.

EXT_CAC_RCT.1 Application and change control react

Hierarchical to: No other components

Dependencies: EXT_CAC_WL.1

EXT_CAC_RCT.1.1 The System shall perform the following analysis function(s) on all application data collected and take the associated action(s) in response [assignment: associated action(s)].

6 Security Requirements (ASE_REQ.2)

6.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 5) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].
- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].
- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.
- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

6.2 Security Functional Requirements

6.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 6.1 above and itemised in the table below.

Identifier	Title
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute-based access control

Identifier	**Title**
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FTP_TRP.1	Trusted Path
EXT_CAC_WL.1	Application and change control data collection
EXT_CAC_RCT.1	Application and change control react

Table 11 – Overview of Security Function Requirements

6.2.2 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
FAU_GEN.1.1	The TSF shall be able to generate an audit report of the following auditable events: ~~a) Start-up and shutdown of the audit functions;~~ b) All auditable events for the [***not specified***] level of audit; and c) [**Specifically defined auditable events listed in the Notes section below**].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, MD5, Path, Command line client computer, Packages, subject identity (if applicable), and the outcome (success or failure) of the event, and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [none].
Dependencies:	FPT_STM.1 Reliable time stamps

Notes:	Auditable events within the TOE: a) Action Logs - Date & time, username, IP Address, Event type (refer to SFR) b) Event Logs - Date & time, MD5, Path, Computer and Packages c) Fileless Logs – Time, Command Line, Computer

6.2.3 FAU_SAR.1 Audit Review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**Super Admin, Admin and Read-Only**] with the capability to read [**all audit information**] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

6.2.4 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**access control SFP**] on [**objects listed in the table below**].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	

Subject	**Object**	**Operation**
Super Admin	Dashboard	Select/View All Branches Server dashboard information
	Manage	Add/Delete/Change/ View list of Branches Add/Delete/Change/ View list of Administrator
	Clients	Select/Import/View client's Group
	Rules	Add/Delete Groups Duplicate Application Rules

			Allow/Disallow Application Rules
		Samples	Export List File Samples Export List Certificate Samples View File Verdicts View Certificate Verdicts
		Logs	Export/View Event Logs Export/View Fileless Logs Export/View Action Logs Generate Report
		Report	Clear/Select/View Branch Select Date Generate Report
		Settings	Website/Proxy/SMTP Configuration Enable/disable Auto Whitelisting Configure Client's Agent Updates Configure Rules, Agent Database and Automatic Whitelisting View License Enable/Disable email to admins when license status changed Configure the Archive Database Update Syslog Configuration Configure Ping Interval
	Admin	Dashboard	Select/View authorised dashboard information
		Branches	Change/ View list Branches View list of users (Super Admin, Admin, Read-Only)
		Clients	Select/Import/View authorised client's Group
		Rules	Add/Delete Groups

			Duplicate Application Rules Allow/Disallow Application Rules
		Samples	Export List File Samples Export List Certificate Samples View File Verdicts View Certificate Verdicts
		Logs	Export/View Event Logs Export/View Fileless Logs Export/View Action Logs
		Report	Clear/Select/View Branch Select Date Generate Report
	Read-Only	Dashboard	Select/View All Branches Server dashboard information
		Branches	View List of Branches View client(s)
		Clients	View client(s)
		Rules	View Allow/Disallow Application Rules
		Samples	Export List File Samples Export List Certificate Samples View File Verdicts View Certificate Verdicts
		Logs	Export/View Event Logs Export/View Fileless Logs Export/View Action Logs
		Report	Clear/Select/View Branch Select Date Generate Report

Table 12 – Access control

6.2.5 FDP_ACF.1 Security attribute-based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**access control SFP**] to objects based on the following: [**as listed in the Notes section of FDP_ACC.1**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a) First Time login, Super Admin, Admin and Read-only user must set their password before performing any action for the first time** **b) Super Admin, Admin and Read-only user user must enter their username and password before performing any action** **c) Super Admin, Admin and Read-only user can change their password once they have authenticated with the TOE**]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**TOE detects User Interface running on existing session, IP Address and devices**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**TOE detects User Interface running on different sessions, IP Address and devices and required termination code to terminate previous session and continue with new session**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

6.2.6 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**Username, Password**]
Dependencies:	No dependencies.
Notes:	None.

6.2.7 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

6.2.8 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies
Notes:	None.

6.2.9 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**access control SFP**] to restrict the ability to [***change_default, modify, delete]*** the security attributes [**Admin Account, Read-Only Account**] to [**Super Admin account**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

6.2.10 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**access control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

6.2.11 FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components.
FMT_MTD.1a.1	The TSF shall restrict the ability to [***manage***] the [**assign users to roles, User ID**] to **[Super Admin]**
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

6.2.12 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**refer to Table 12**].
Dependencies:	No dependencies.
Notes:	None.

6.2.13 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**Super Admin, Admin and Read-Only**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

6.2.14 FTP_TRP.1 Trusted Path

Hierarchical to:	No other components.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification or disclosure***].
FTP_TRP.1.2	The TSF shall permit [***remote users***] to initiate communication via the trusted path
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [***initial user authentication***, [**and all further communication after authentication**]].

Dependencies:	No dependencies
Notes:	None

6.2.15 EXT_CAC_WL.1 Application and change control data collection

Hierarchical to:	No other components.
EXT_CAC_WL.1.1	The TSF shall be able to collect the following information from the targeted client system resources: [**For application control:** **a) A whitelist inventory of program code, including binary executables command line and scripts;** **b) Events indicating prevented unauthorized executions of program code;**]
EXT_CAC_WL1.2	At a minimum, the System shall collect and record the following information: [**a) For application control:** **The Application Name (the application that is performing the action) and the Object Name (the object that is being acted upon);**]
Dependencies:	No dependencies
Notes:	None

6.2.16 EXT_CAC_RCT.1 Application and change control react

Hierarchical to:	No other components.
EXT_CAC_RCT.1.1	The System shall perform the following analysis function(s) on all application data captured and take the associated action(s) in response: [**For application control:** **a) Compare the application rules of any client application attempting to execute to an on the client with the whitelist to determine whether it has permission.**]
Dependencies:	EXT_CAC_WL.1
Notes:	None

6.3 Security Requirements Rationale

6.3.1 Dependency rationale

Below demonstrates the mutual supportiveness of the SFR's for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE, and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level EAL2 as defined in Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

SFR	Dependency	Inclusion
FAU_GEN.1	FPT.STM.1 Reliable time stamps	FPT_STM.1 has not been included as the TOE obtains all audit timestamps from the underlying platform. This has been addressed in Section 3.4 by A.TIMESTAMP.
FAU.SAR.1	FAU.GEN.1 Audit data generation	FAU.GEN.1
FDP_ACC.1	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_ATD.1	No dependencies	NA
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1

SFR	Dependency	Inclusion
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FTP_TRP.1	No dependencies	N/A
EXT_CAC_WL.1	No dependencies	N/A
EXT_CAC_RCT.1	EXT_CAC_WL.1 Application and change control data collection	EXT_CAC_WL.1

6.3.2 Mapping of SFRs to security objectives for the TOE

Security objective	Mapped SFRs	Rationale
O.USER	FIA_UAU.2	The requirement helps meet the objective by authenticating user before any TSF mediated actions.
	FIA_UID.2	The requirement helps meet the objective by identifying user before any TSF mediated actions
O.ACCESS	FAU_GEN.1	This SFR specifies security events that are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. It traces back to this objective.
	FAU_SAR.1	This SFR specifies that Super Admin, Admin and Read-Only will have the capability to view the audit trail data in log form. It traces back to this objective
	FIA_ATD.1	The requirement helps meet the objective by ensuring user security attributes are maintained.
	FMT_SMF.1	The requirement helps meet the objective by providing management functions of the TOE for authenticated user.
	FMT_SMR.1	The requirement helps meet the objective by providing user timing of identification.
	EXT_CAC_WL.1.1	The requirement helps meet the objective by ensuring unauthorised or malicious application to not execute on client computer.

Security objective	Mapped SFRs	Rationale
O.MANAGE	FMT_MTD.1	The requirement helps meet the objective by restricting the ability to modify the user password.
	FMT_MSA.1	The requirement helps to meet the objective by restricting the ability to modify the security attributes for the Super Admin.
	EXT_CAC_RCT.1.1	The requirement helps meet the objective by providing application captured and take the associated action(s) in response.
O.CONFIG	FMT_MTD.1	The requirement helps meet the objective by restricting user access to management functions.
	FMT_MSA.1	The requirement helps meet the objective by restricting user access to security attributes.
	FMT_MSA.3	The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP.
	FMT_SMR.1	The requirement helps meet the objective by defining the security roles used within the TOE.
	FDP_ACC.1	The requirement provides access control functionality to ensure that access to security functionality is controlled.
	FDP_ACF.1	The requirement provides access control functionality to ensure that access to security functionality is controlled.
O. SEC_COM	FTP_TRP.1	The requirement ensures that data sent by users is protected from modification or disclosure.

7 TOE Security Assurance Requirements (ASE_REQ.2)

7.1 Overview

EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements

Assurance class	Assurance components
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7.2 Justification for SAR selection

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2).

TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

8 TOE Summary Specification (ASE_TSS.1)

8.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE implements the claimed security functional requirements. The TOE provides the following security functions:

- Application Control (Whitelist);
- Audit;
- Identification and Authentication;
- Security Management; and
- Secure Communication

8.2 Application Control (Whitelist)

The TOE will prevent implement executing unauthorized application, unknown application, malware and zero-day malware on client (EXT_CAC_WL.1.1). The TOE can be configured to allow authorised application to execute on client to prevent execution of unauthorized application, unknown application, malware and zero-day malware (EXT_CAC_RCT.1.1).

8.3 Audit

The TOE will create audit records (which contain the data and time of the event, type of event, subject identity and outcome of the transaction event) for the following auditable events (FAU_GEN.1):

a) Action Logs - Date & time, username, IP Address, Event type (refer to SFR)
b) Event Logs - Date & time, MD5, Path, Computer and Packages
c) Fileless Logs – Time, Command Line, Computer

The TOE's Super Admin, Admin and Read-Only have the capability to review these audit records via the software interface (FAU_SAR.1). Timestamps for the server are generated for audit logs by utilising the underlying operating system. The TOE does not generate its own timestamps for use in audit records; these are supplied by the underlying operating system.

8.4 Identification and Authentication

The TOE implements access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (FDP_ACC.1). All TOE users must provide authentication data to the TOE to affirm their identity and role prior to being granted access to any TOE functions or interfaces.

The TOE maintains three (3) types of users which are Super Admin, Admin and Read-Only user (FMT_SMR.1). These users may access the TOE via the web interface that the platform provides. TOE user must be authenticated to the TOE prior performing any TOE functions by entering a username and password (FIA_ATD.1a, FIA_UAU.2, FIA_UID.2, FDP_ACF.1). Upon first time login to the server Super Admin, Admin and Read-Only user must set their new password before performing any action (FDP_ACF.1).

8.5 Security Management

The TOE provides a suite of management functions only to Super Admin and Admin. These functions allow for the configuration of TOE to suit the environment in which it is deployed in centralise management and/or branches. Additionally, management roles may perform the following tasks (FMT_SMF.1, FMT_MTD.1, FMT_MSA.1 and FMT_MSA.3):

Roles	Menu	Operation
Super Admin	Dashboard	Select/View All Branches Server dashboard information
	Manage	Add/Delete/Change/ View list of Branches Add/Delete/Change/ View list of Administrator
	Clients	Select/Import/View client's Group
	Rules	Add/Delete Groups Duplicate Application Rules Allow/Disallow Application Rules
	Samples	Export List File Samples Export List Certificate Samples View File Verdicts View Certificate Verdicts
	Logs	Export/View Event Logs Export/View Fileless Logs Export/View Action Logs Generate Report
	Report	Clear/Select/View Branch

		Select Date Generate Report
	Settings	Website/Proxy/SMTP Configuration Enable/disable Auto Whitelisting Configure Client's Agent Updates Configure Rules, Agent Database and Automatic Whitelisting View License Enable/Disable email to admins when license status changed Configure the Archive Database Update Syslog Configuration Configure Ping Interval
Admin	Dashboard	Select/View authorised dashboard information
	Branches	Change/ View list Branches View list of users (Super Admin, Admin, Read-Only)
	Clients	Select/Import/View authorised client's Group
	Rules	Add/Delete Groups Duplicate Application Rules Allow/Disallow Application Rules
	Samples	Export List File Samples Export List Certificate Samples View File Verdicts View Certificate Verdicts
	Logs	Export/View Event Logs Export/View Fileless Logs Export/View Action Logs

	Report	Clear/Select/View Branch Select Date Generate Report

The TOE implements access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (FDP_ACC.1 and FDP_ACF.1).

8.6 Secure Communication

When a user accesses the TOE on their browser, by typing in the website address, the TOE will initiate a TLS secure channel establishment with the user's browser by utilizing Transport Layer Security (TLS v1.2) protocols (FTP_TRP.1)