MOzART Command Center Web Portal
Security Target

CERTIS CISCO SECURITY PTE LTD

Evaluation Assurance Level 2

Version 1.26

11 May 2021

CONFIDENTIAL

Document Details

Version	Date	Description	Author
1.0	21 October 2019	Security Target (ST) generated with required document template	Zhang Tianxia
1.2	21 November 2019	Added Chapter 1 to Chapter 4	Ann Kuen Go
1.3	28 November 2019	Review and updated Chapter 1 to Chapter 4	Zhang Tianxia and Consultant
1.4	06 December 2019	Added Chapter 5 and 6	Ann Kuen Go
1.5	20 December 2019	Review and updated Chapter 5 and 6	Zhang Tianxia and Consultant
1.6	08 January 2020	Changed TOE Version from 2.0 to 1.1 Reworked on Chapter 1 to 4	Ann Kuen Go
1.7	17 January 2020	Reviewed changes of Chapter 1 to 4	Zhang Tianxia and Consultant
1.8	21 January 2020	Reworked Chapter 5 and 6 Added Chapter 7 Security Functional Requirement	Ann Kuen Go
1.9	23 January 2020	Reviewed Chapter 7 Review changes of Chapter 5 and 6	Zhang Tianxia and Consultant Anthony Chan
1.10	27 February 2020	Added additional information into Chapter 7	Ann Kuen Go
1.11	03 March 2020	Reviewed changes of Chapter 7 Reviewed and confirmed changes of Chapter 1 t0 4	Zhang Tianxia and Consultant
1.12	06 March 2020	Added additional information into Chapter 7	Ann Kuen Go
1.13	10 March 2020	Reviewed and confirmed changes of Chapter 7 Reviewed and confirmed changes of Chapter 5 and 6	Zhang Tianxia and Consultant
1.14	13 March 2020	Added Chapter 8 Security Assurance Requirements	Zhang Tianxia and Consultant
1.15	15 March 2020	Review Chapter 8 Added Chapter 9 TOE Summary Specification	Ann Kuen Go
1.16	16 March 2020	Reviewed Chapter 9 Added additional information into Chapter 8	Zhang Tianxia and Consultant
1.17	17 March 2020	Updated Chapter 9 Reviewed and confirmed changes of Chapter 8	Ann Kuen Go
1.18	18 March 2020	Reviewed changes of Chapter 9 Confirmed Chapter 9	Zhang Tianxia and Consultant
1.19	19 March 2020	Finalized the document	Anthony Ann Kuen Go Zhang Tianxia Consultant
1.20	12 Aug 2020	Amended Administration list under the Chapter 9.5 User Data Protection Removed - Event-Camera Mapping - Event Classification - Camera Plotting Added - Equipment Event Mapping - Guard Tour	Ann Kuen Go

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

1.21	14 August 2020	Amended Administration list under the Chapter 9.5 User Data Protection Added - Virtual Patrol	Ann Kuen Go
1.22	23 October 2020	Updated document as per EOR Report	Ann Kuen Go
1.23	11 November 2020	Amended document content base on consutant feedback	Ann Kuen Go
1.24	23 November 2020	Updated application note in section 7.2	Ann Kuen Go
1.25	07 May 2021	Aligned the terms used in the document according to ADV EOR	Ann Kuen Go
1.26	11 May 2021	Updated feedbacks in EOR	Ann Kuen Go

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

TABLE OF CONTENTS

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

1 SECURITY TARGET INTRODUCTION (ASE_INT.1)

This section identifies information as below:

- Security Target (ST) and Target of Evaluation (TOE) reference
- Document Organization

1.1 SECURITY TARGET (ST) AND TARGET OF EVALUATION (TOE) REFERENCE

ST Title	Certis - MOzART Command Center Web Portal Security Target Documentation (EAL 2)-v1.26
ST Identifier	MOzART-Command-Center-Web-Portal_ST_EAL2_v1.26
ST Version/Date	v1.26, 11 May 2021
TOE Title	MOzART Command Center Web Portal
TOE Version	Version 1.1
TOE Date of Release	3 October 2019
Assurance Level	Evaluation Level Assurance 2 (EAL2)
CC Identification	Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5 • Part 1: Introduction and General Model • Part 2: Security Functional Components • Part 3: Security Assurance Components Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 5 Evaluation Methodology

1.2 DOCUMENT ORGANISATION

This document is divided into the following major sections:

1. Security Target (ST) Introduction
2. Target of Evaluation (TOE) Overview
3. Conformance Claims
4. Extended Components Definition
5. Security Problem Definition
6. Security Objectives and Rationale
7. Security Functional Requirements (SFR) and Rationale
8. Security Assurance Requirements (SAR)
9. Target of Evaluation (TOE) Summary Specification

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

2 TOE OVERVIEW

The Target of Evaluation (TOE) is a web-based application portal called the **MOzART Command Center Web Portal (MOzART CC)** which provides TOE users means of monitoring, operating, managing and administering physical security incidents through the **Intranet** (private network). Fundamentally, the TOE can be accessed by consumers via any web browser with JavaScript capabilities that supports the JavaScript ES7 components (front-end Command Center) as long as the consumers are residing in the same private network as the TOE.

2.1 TOE USAGE AND MAJOR SECURITY FEATURES

The target audience of the ST encompasses TOE users who are interested in maintaining and controlling physical security. The MOzART CC allows consumers to have a "one-to-all" control over many integrated physical security appliances such as fire alarm triggers, surveillance cameras, parameter sensors and entry alarm triggers around a designated premise. However, the TOE itself can only be accessed via a private network deployed within the TOE user's premises. All modules/functions on the same private network related to the querying of live data, feeds by the third-party APIs (supporting non-TOE software) and displayed by the TOE will not require Internet connection.

The TOE is capable of the performing the following upon successful authentication:

Modules	Descriptions
Case Dashboard	• Access to main UI page primarily used by operators to view incoming alarm events • To manage workflow and lifecycle of these events.
Map UI	• Interactive building/site map that gives users visualization and situational awareness in the remote site. • Displays the location cameras, staff, sensors, and other devices.
Live View	• Displays a collection of CCTV cameras grouped per building/site that allows users to view live video feeds.
Incident Management	• Used to assign, create, report and query incidents or cases remotely. • The ability to pinpoint and instruct the nearest possible security personnel to investigate an incident.
Active Events	• Real-time events are queried and displayed based on live footages and feeds from multiple integrated physical security appliances and reports from security personnels.
Duty Roster (or Task Scheduling)	• Allows supervisors to manage users, staffs and security personnels' scheduled tasks. • Tasks are scheduled based on map view of a given premise (blueprint-based). • Tasks are not scheduled based on the relations to a case.
Event Filters	• Filter function to categorize and prioritize desired events.
Argus Guard Tour	• Integrated function with capabilities of identifying security personnel's current physical location and patrolling routes.
Case Search	• Identify cases based on filtered queries.

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

Reporting and Documenting	• Report production and generation used for incident frequency tracking and summary over a given span of time.
Virtual Patrol	• The function to access through third-party integrated surveillance cameras based on each interval set to closely simulate a physical guard patrol duty remotely. • Blueprints of a premise are added into the MOzART CC to identify location of patrol coverage. • Used to create a virtual patrol sequence. • A functional module that allows users to monitor remote site situation via CCTV cameras and report unusual activities or abnormal situations. This is comparable to a roving team on-site but without the physical presence of the monitoring staff.
Calendar of Events	• Shows pass incidents that have occurred.
Administration	• Allows administrator and supervisor to manage master data such as case types, building maps, etc. • Provides special administrative functions such as searching previous cases and modifying closed cases that are otherwise unavailable to normal operators.

Table 1 shows modules available to user with appropriate role(s) after successful authentication

In a summary, the MOzART CC is a highly sophisticated Command Center, acting as the main user interface for TOE users (in their respective roles as an operator, supervisor or administrator) to monitor events, operate cases, manage cases, and administer the MOzART CC itself. The rest of the components within the MOzART system (platform, server, database, CEP, business components) and integrated third-party security appliances, devices, APIs are deemed as out of the TOE scope.

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

The TOE, MOzART CC provides the following security features, which are being claimed for this evaluation:

- Identification and Authentication
- Security Audit
- Trusted Path/Channels
- User Data Protection

2.2 SUPPORTING NON-TOE HARDWARE

The MOzART system is supported by 3 supporting non-TOE Hardware (Table 2) which provisions the 6 major components as listed below:

- Mozart Portal (TOE)
- Media Server
- Mozart API Services
- CEP
- Certis Secure Mobile App
- SQL Server

The supporting non-TOE hardware is also extended to the integrated third-party APIs which feeds data to the TOE.

The following are categorized as out of scope from the selected TOE:

- Database server
- web application server
- application server

The table below denotes the minimum specification for the respective system to run in support of the TOE

Hardware	Minimum Specification
Database Server	OS: Windows Server 2016 MongoDB and SQL 2017 CPU: 4 cores RAM: 8GB Disk Space: 200GB
Web Application Server	OS: Windows Server 2016 CPU: 4 cores RAM: 8GB Disk Space: 20GB
Application Server	OS: Windows Server 2016 CPU: 4 cores RAM: 4GB Disk Space: 20GB

Table 2 shows the out-of-scope components from the TOE

The following describes the minimum number of Windows-hosted virtual machines created to support the TOE:

Servers	Quantity
Web Application Server	1
Application Server	1
Database Server	1

Table 3 shows number of virtual machines needed to support the TOE

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

2.3 SUPPORTING NON-TOE SOFTWARE

The MOzART system is comprised of 6 major components (depicted as yellow boxes in the image below). Out of these 6 major components, 5 of them (including the uncolored boxes) are deemed as supporting non-TOE software. The rest of the uncolored boxes fall into the category of smaller sub-components and other third-party APIs.

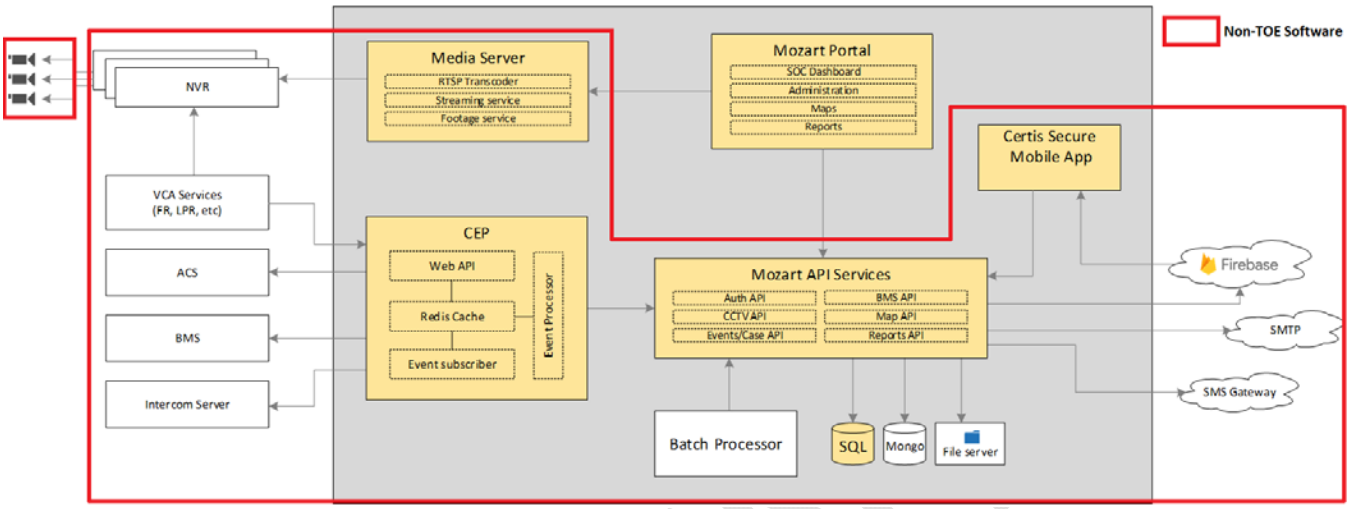


Figure 1 shows the supporting non-TOE software shown within the red boxes above.

Software	Version	Description
Media Server	v1.1	Comprised of 3 sub-components, the media server is mainly responsible for converting CCTV video streams from different types of cameras and/or streaming protocols into a series of images for further processing. • **RTSP transcoder** – converts video stream into a series of images • **Streaming Service** – uses the websocket protocol to deliver the images to websocket clients • **Footage Service** – stores the series of images into a persistent storage when requested.
CEP	v1.1	Main interface touchpoint with external devices such as sensors and camera triggers. CEP provides 2 modes of interfacing: • **Web API** (inbound connection) – for static devices or external applications that can trigger web API calls to send data • **Event subscription** (outbound connection) – for external devices that only provides inbound connections such as streams, OPC, or web APIs. CEP will establish the connection to the external device and wait for messages. As CEP is expected to receive thousands or probably millions of messages in a second, Redis acts as both cache manager (for performance) and message broker (for reliability). The **Event Processor** component then aggregates, filters, and transforms the message accordingly and transmit the data into MOzART.
API Services	v1.1	The core of MOzART. Consists of several RESTful-based APIs that provides data and functional processing logic.

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

MOzART Command Center Web Portal	MOzART Command Center Web Portal Version 1.1	The main user interface for operators and supervisors to monitor events, operate, manage cases, and administer the MOzART system. It is built purely using HTML 2.0, CSS 3, and Javascript ES 7. **This is the TOE itself**.
Microsoft Authenticator Application	iOS version 6.5.4 Android version 6.2010.6717	The 2FA application that generates the token needed to gain access to the TOE after the user has successfully authenticated themselves using the user name and password
Database Server	Microsoft SQL Server 2017 (RTM-GDR) (KB4505224) - 14.0.2027.2 (X64) Standard Edition (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393) (Hypervisor)	MOzART uses Microsoft SQL Server 2016 relational DB as persistent storage.
STS Portal	v1.1	STS Portal is a separate web application for managing MOzART Users and Clients. It provides only 4 main purposes: • **User management** – allows administrators to manage users and roles. Administrators can add, delete, activate, deactivate, and change passwords of the users. • **Client management** – allows administrators to manage MOzART clients. Clients can be devices, internal or external applications. Clients can have 2 authentication modes: o **API-key authentication** – key-based authentication that can be used to access MOzART API services without having a client credential. This is more applicable to static devices that can only support outgoing web API calls. o **OAuth2 client credential flow** – similar to User Name/password flow, the client credential flow provides more security by generating short-lived JWT bearer tokens. Administrators can add, delete clients as well as assign API-Key or update client secret. • **Refresh Token Management** – allows administrators to invalidate refresh tokens. Refresh tokens are long-lived tokens that can be used by clients to request new access tokens without the need to specify again the User Name/password or client id/secret combination. In the case where the refresh token is compromised, administrators can delete the refresh token to invalidate it.
Third-party APIs	Gallagher Command Centre version EL8.10.1 XJera Analyst version 1.0.3.0 Argus CC version 20191119	• **Gallagher Command Centre** – provides building alarm events. TOE establishes outbound HTTPS connection to the Gallagher API. • **XJera Analyst** – provides VCA-related events. XJera connects to the TOE's API services. • **Argus CC** – backend platform of the Argus Mobile devices

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

2.4 CLIENT REQUIREMENTS

The respective JavaScript Components (ES 7) consists of the following for the TOE to work as intended:

- jQuery 3
- AngularJS
- Bootstrap
- ChartJS
- JS Widgets
- WebSockets

Hence, any web browser with JavaScript capabilities that supports the JavaScript ES7 components will be able to access the TOE's full functionality as intended (within the same network link). With that said, both JavaScript and web cookies must be enabled to facilitate web portal sign-ins.

The TOE directly utilizes the supporting non-TOE API Services and Video Stream components when retrieving data transmitted through a secure communications channel, Hyper Text Transfer Protocol Secure (HTTPS) and secure websockets which leverages on Transport Layer Security (TLS).

2.5 TOE DESCRIPTION

2.5.1 Physical Scope of the TOE

The TOE is a web-based application portal which provides TOE users means of monitoring, operating, managing and administering physical security incidents through the **Intranet** (private network). Fundamentally, the TOE can be accessed by consumers via any web browser with JavaScript capabilities that supports the JavaScript ES7 components (front-end Command Center) as long as the consumers are residing in the same private network as the TOE. The physical server that hosts the TOE is managed by the TOE user's infrastructure team. The rest of the components within the MOzART system (platform, server, database, CEP, business components) including integrated third-party security appliances, devices and APIs are deemed as out of the TOE scope.

TOE users are able to access the TOE upon successful authentication through the web browser and perform the TOE's intended operations. Both installation and setup are required to bring up the TOE to an operational state before being authenticated through the TOE to access the functions of the TOE.

The Section 3 of Operational User Guidance ([AGD_OPE.1] MOzART CC EAL2 - Operational User Guidance.docx) and Deployment Process section in Preparative Procedure ([AGD_PRE.1] MOzART CC EAL2 – Preparative Procedure.docx) documents serve as a guide for user to refer to in the event of operation or system issue.

The diagram below depicts the entire MOzART system architecture. The TOE within this Security Target documentation is described and marked as the following below:

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

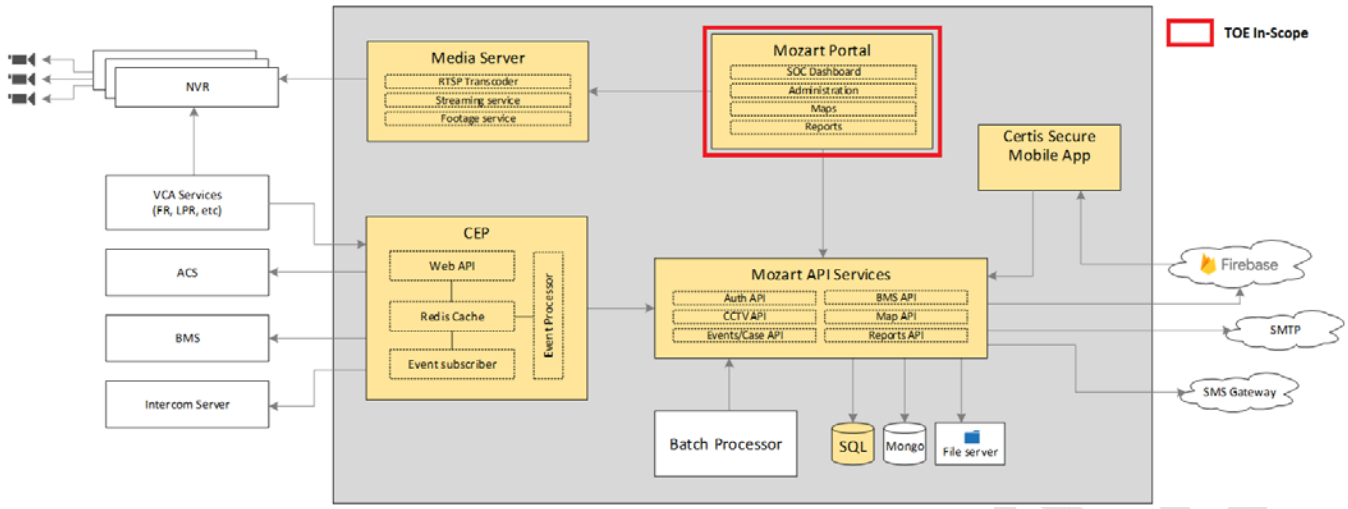


Figure 2 shows the MOzART system architecture, with physical scope of the TOE, MOzART Command Center Web Portal boxed in red above.

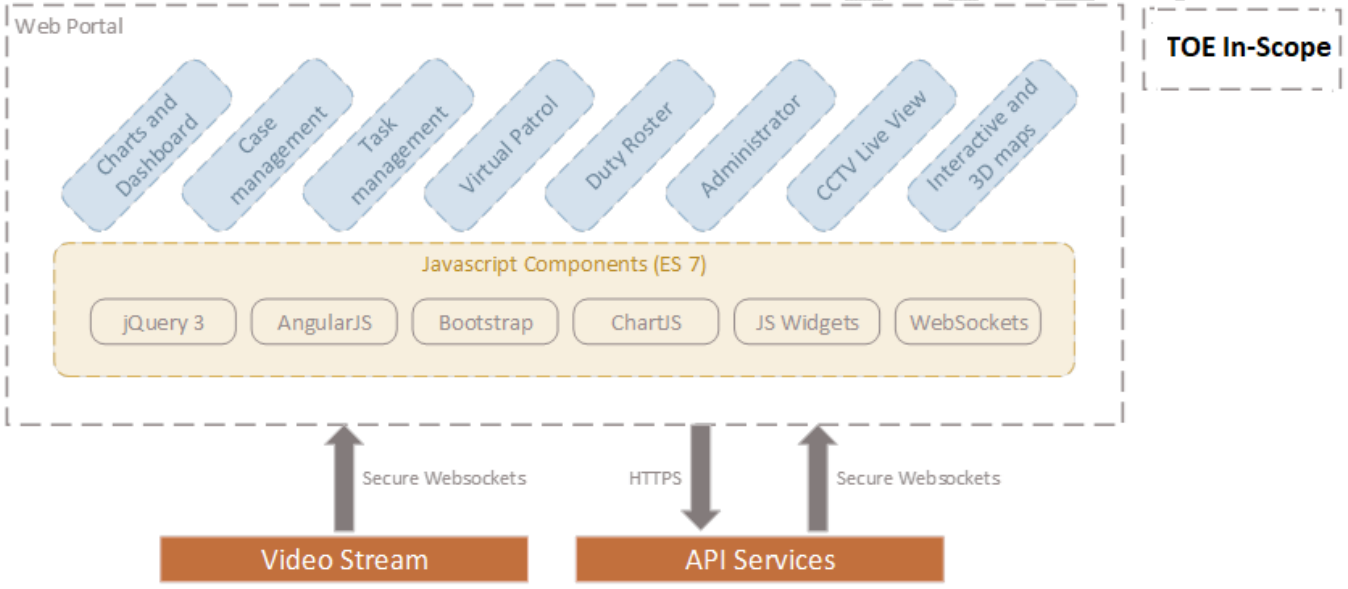


Figure 3 shows the detailed application architecture together with the physical scope of the TOE boxed in dotted lines. Both Video Stream and API Services are deemed as out of scope.

All hardware appliances/devices, software components and integrated third-party physical security appliances and APIs used to support the TOE are not part of the scope of evaluation. Every other component that is not boxed in the above diagrams (refer to Figure 1 and Figure 2) are considered not in-scope. All non-TOE components mentioned within the supporting non-TOE hardware and supporting non-TOE software section (see page 8 – 12) are required for the TOE to function as intended.

The TOE in-scope provides the access and usage of the MOzART CC modules and functions directly. The TOE's main usage provides TOE users means of monitoring, operating, managing and administering physical security incidents. The target audience of the ST encompasses consumers who are interested in maintaining and controlling physical security. The MOzART CC allows consumers to have a "one-to-all" control over many integrated physical security appliances such as fire alarm triggers, surveillance cameras, parameter sensors and entry alarm triggers around a designated premise.

The TOE can only be used by authenticated users via web browser. Customers will need to obtain the administrative privilege account from the Certis Deployment Team in order to use the TOE from the beginning. Subsequent TOE user accounts are created and managed by the TOE users from a separate application (supporting non-TOE software).

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

Prior to the operational state of the TOE, both delivery and preparative procedures must be fulfilled. In conjunction to the preparative procedures, Certis Deployment Team will be in charge of performing the relevant supply and delivery of supporting non-TOE hardware to the TOE user's premises before the installation of supporting non-TOE software takes place. Once the delivery of the product is complete, the installation and configuration of supporting non-TOE software, relevant components and the TOE (MOzART CC) will be carried out by the Certis Deployment Team on the TOE user's premises. From here on, the TOE users (based on their respective organization's roles) will be given control to manage the physical server hosting the TOE.

The TOE deployment (for all delivery, installation and configuration) will be the sole responsibility of Certis Deployment Team. The following are a summary of steps taken to see through it that the TOE is properly sent, configured and responds accordingly to the expected operational state:

1. Procurement of physical servers (supporting non-TOE hardware),
2. Creation of Windows-hosted virtual machines (supporting non-TOE software):
    a. x1 web server,
    b. x1 application server; and
    c. x1 database server.
3. Installation of prerequisite supporting non-TOE software (SQL server, IIS, .NET framework);
4. Installation and configuration of TOE.

In a similar scenario, the consumers are given the option to provide their own supporting non-TOE hardware. Regardless, the creation of virtual machines, installation of prerequisites (supporting non-TOE components) and configuration of the TOE will be conducted within consumer's premises.

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

2.5.2 Logical Scope of the TOE

The TOE provides the following security features:

Security Features	Descriptions
Identification and Authentication	Authentication mechanism in place • TOE identifies and authenticates users before the users are allowed to perform any actions within the TOE. • The TOE is capable of handling security concerns over the use of User Name/password credentials combination to authenticate through the MOzART Command Center Web Portal (MOzART CC). • The TOE has a set of password rule and policies which strengthens the complexity of an authentication. • The TOE has a 2-factor authentication mechanism in place.
Security Audit	Audit event logs • TOE generates the audit logs and stores them in a non-TOE location for the auditable events. The actions taken for viewing the audit logs and audit logs review process are out of the TOE scope. • The TOE has several levels of audit trails and events enabled within the TOE. • The auditable events that will be logged by the TOEare as below: o The starting and stopping of TOE o User authentication process, i.e. the TOE's security audit trail records the login attempts of a TOE user o All TOE user actions inside the TOE such as: ▪ Create record ▪ Delete record ▪ Update record
Trusted Path/Channels	Secure communications protocol • TOE establishes secured and encrypted communication for incoming and outgoing data transfer of the TOE. • The TOE uses encrypted communication means to exchange data.
User Data Protection	Role-based access controls • TOE manages access control policy to ensure user data are only accessible by authorized personnel. • The ability of the TOE to differentiate user roles and responsibilities accurately by addressing any security flaws.

Table 4 shows the Security Functions of the TOE

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

3 CONFORMANCE CLAIMS (ASE_CCL.1)

3.1 COMMON CRITERIA CONFORMANCE CLAIM

This ST and TOE are conformant to version 3.1 (Revision 5) of the Common Criteria for Information Technology Security Evaluation. Specific conformance claims are as below:

- **Part 2 conformant.**
  Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, version 3.1 (Rev 5).
- **Part 3 conformant.**
  Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, version 3.1 (Rev 5).

3.2 PROTECTION PROFILE CLAIMS

This ST does not claim conformance to any Protection Profile.

3.3 PACKAGE CLAIMS

The ST is conformant to EAL 2 assurance package as defined in Part 3 of Common Criteria version 3.1 (Rev 5).

3.4 CONFORMANCE CLAIMS RATIONALE

No conformance claims rationale is necessary as this ST does not claim conformance to Protection Profile.

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

4 EXTENDED COMPONENTS DEFINITION (ASE_ECD.1)

This TOE does not consist of any extended components, hence the requirements for the Extended Components Definition (ASE_ECD) are not applicable.

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

5 SECURITY PROBLEM DEFINITION (ASE_SPD.1)

This section describes the nature of security problem that are intended to be addressed by TOE, which is described through:

- Known or assumed threats which TOE shall address.
- Organizational security policies that specify rules or guidelines for TOE users to comply with.
- Assumptions about the security aspects of the environment which TOE is intended to operate.

5.1 THREATS

The followings are the threats identified for TOE. TOE is responsible for addressing the threats to the environment where it resides.

Threat Identifier	Threat Statement
T.BROKEN_AUTH	An unauthenticated individual may attempt to bypass the authentication function to access the TOE's primary functions and data.
T.UNAUTHORIZED_ACCESS	An authenticated individual may attempt to bypass assigned privileges to access unauthorized TOE data, functions, configurations or restricted information.
T.INTERCEPTION	An arbitrary individual may sniff or intercept the communication channel where sensitive data are being transmitted between the TOE and the TOE user's web browser.

Table 5 shows the threats identified for the TOE

5.2 ORGANIZATIONAL SECURITY POLICIES

The followings are the Organizational Security Policies (OSP) expected to be imposed by an organization to secure the TOE and its environment.

OSP Identifier	OSP Statement
P.PASSWORD	Authorized TOE users are required to use a combination of credentials (User Name and password) where the attribute of the password consists of (at least one) uppercase, lowercase, alphanumeric, special character [<space>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~)] (extended ASCII codes are not allowed) and a minimum length of 8 characters.
P.ACCESS_ROLE	Only authorized individuals that have been assigned with Administrator, Supervisor and Operator roles will be approved of access to the TOE and permitted to perform the corresponding functions of the TOE.
P.CRYPTO	The TOE only accepts secure communications protocol (TLSv1.2 and above) coupled together with a series of secure cipher suites and algorithms when performing data transmission between the TOE and TOE users through a HTTPS connection.

Table 6 shows the Organizationals Security Policies to be imposed by the TOE

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

5.3 ASSUMPTIONS

The following assumptions describes the security aspect of TOE and operational environment where the TOE is deployed.

Assumption Identifier	Assumption Statement
A.ADMINISTRATOR	The assumption is made that the authorized TOE administrators are competent with suitable training provided and are trustworthy individuals allowed to accept the role of configuration and management of the TOE.
A.TIMESTAMP	The assumption is made that the platform on which the TOE operates shall be able to provide reliable and synchronized timestamps across the MOzART system to preserve accurate audit logs.
A.PHYSICAL_ENVIRONMENT	The assumption is made that the TOE and its platform are located within secured facilities with controlled access to prevent unauthorized physical access.
A.MALWARE	The assumption is made that the platform on which the TOE operates shall be protected against malware.
A.DDOS	The assumption is made that WAF (Web Application Firewall) will be a standard deployment in the TOE's operational environment to guard against DDoS attacks.
A.THIRDPARTY	The assumption is made that all integrated third-party data communicated between the TOE maintains integrity.

Table 7 shows the Assumptions applied to the TOE

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

6 SECURITY OBJECTIVES (ASE_OBJ.2)

This section provides the security objectives which address the threats, assumptions and Organizational Security Policies as per described in earlier chapter “Security Problem Definition”.

6.1 SECURITY OBJECTIVES FOR TOE

This sub-section describes the relationship between the security objectives for the TOE and the security problem definitions.

Security Objectives Identifier	Objective Statement and Security Problem Definition Mapping
O.SEC_ACCESS	Objective Statement The TOE shall ensure that only authorized individuals are able to access protected resources, functions, configurations and to explicitly deny access to specific individuals when a resource access is beyond the assigned privilege. SPD Mapping Threat: T.UNAUTHORIZED_ACCESS OSP: P.ACCESS_ROLE
O.SEC_AUTHENTICATE	Objective Statement The TOE shall ensure that the security mechanisms are in place to increase the difficulty of unauthenticated access such as brute force attempts and login bypasses made by arbitrary individuals. SPD Mapping Threat: T.BROKEN_AUTH OSP: P.PASSWORD
O.SEC_COMMUNICATION	Objective Statement The TOE shall ensure that secure communications channels and secure cipher suites and algorithms are being implemented to protect data sent between the TOE and the TOE users. SPD Mapping Threat: T.INTERCEPTION OSP: P.CRYPTO

Table 8 shows security objectives for the TOE and the security problem definitions

6.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT

This sub-section describes the relationship between the security objectives for the operational environment and the security problem definitions.

Security Objectives Identifier	Objective Statement and Security Problem Definition Mapping
OE.ADMINISTRATOR	Objective Statement The owners of the TOE must ensure that the administrator who manages the TOE is non-hostile, competent and applies all administrative guidance in a trusted manner. SPD Mapping

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

	Assumption: A.ADMINISTRATOR
OE.SYN_TIMESTAMP	Objective Statement A reliable timestamp is maintained and provided by the operational environment for the TOE in conjunction with the Network Time Protocol (NTP) synchronization. SPD Mapping Assumption: A.TIMESTAMP
OE.SAFE_PHYSICAL_ENV	Objective Statement The TOE must be installed and operated in a physically secured area. SPD Mapping Assumption: A.PHYSICAL_ENVIRONMENT
OE.ANTI_MALWARE	Objective Statement The devices that are accessing to the TOE platform should be guarded against malware and viruses and only trusted and scanned removable devices are able to be plugged in to the servers used by the TOE. All servers used by the TOE should also be installed with an antivirus software. SPD Mapping Assumption: A.MALWARE
OE.ANTI_DDOS	Objective Statement The network that TOE platform resides should be protected with firewalls with the capabilities of blacklisting IPs that are attempting denial of service attacks. SPD Mapping Assumption: A.DDOS
OE.THIRDPARTY	Objectve Statement The TOE accepts all integrated third-party data that maintains its integrity and nonrepudiation. SPD Mapping Assumption: A.THIRDPARTY

Table 9 shows security objectives for the operational environment of the TOE

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

6.3 SECURITY OBJECTIVES RATIONALE

This section explains how security objectives are related to each other. The following table shows threat, organizational security policy and assumptions being mapped to security objectives.

6.3.1 Security Objectives Rationale Summary

	SECURITY PROBLEM DEFINITION (THREATS/ OSPS/ ASSUMPTIONS)										
SECURITY OBJECTIVES	**T.BROKEN_AUTH**	**T.UNAUTHORIZED_ACCESS**	**T.INTERCEPTION**	**P.ACCESS_ROLE**	**P.PASSWORD**	**P.CRYPTO**	**A.ADMINISTRATOR**	**A.TIMESTAMP**	**A.PHYSICAL_ENVIRONMENT**	**A.MALWARE**	**A.DDOS**	**A.THIRDPARTY**
O.SEC_ACCESS		✓		✓								
O.SEC_AUTHENTICATE	✓				✓							
O.SEC_COMMUNICATION			✓			✓						
OE.ADMINISTRATOR							✓					
OE.SYN_TIMESTAMP								✓				
OE.SAFE_PHYSICAL_ENV									✓			
OE.ANTI_MALWARE										✓		
OE.ANTI_DDOS											✓	
OE.THIRDPARTY												✓

Table 10 shows the mapping between Security Objectives and Security Problem Definition

✓ indicates successful mapping of security problem definition and security objective.

6.3.2 Rationale for Security Objectives Mapped to Threats

Threats	Security Objectives	Rationale
T.UNAUTHORIZED_ACCESS	O.SEC_ACCESS	The security objective ensures that the TOE allows authorized individuals only such as TOE Administrator and TOE Supervisor to access TOE configuration data and manage master data functions. Operator on the other hand will be denied of access when he/she tries to

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

		access the function where he/she does not have access/privilege to.
T.BROKEN_AUTH	O.SEC_AUTHENTICATE	This security objective ensures the user is properly authenticated before the individual is allowed to access the TOE.
T.INTERCEPTION	O.SEC_COMMUNICATION	The security objective ensures that the TOE data is being protected and secured during transmission from or to the TOE.

Table 11 shows the rationale for the Security Objectives and its threats

6.3.3 Rationale for Security Objectives Mapped to OSPs

OSPs	Security Objectives	Rationale
P.ACCESS_ROLE	O.SEC_ACCESS	This security objective ensures that the OSP is satisfied by restricting user access based on the roles assigned to Administrator, Supervisor and Operator.
P.PASSWORD	O.SEC_AUTHENTICATE	The security objective ensures that the OSP is satisfied by implementing and enforcing secure password policy.
P.CRYPTO	O.SEC_COMMUNICATION	The security objective ensures that the OSP is satisfied by the usage and enforcement of secure communications protocol of utilizing TLS version 1.2 and above, secure cipher suites and algorithms.

Table 12 shows the rationale for the Security Objectives and its OSPs

6.3.4 Rationale for Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
A.ADMINISTRATOR	OE.ADMINISTRATOR	The security objective counters this assumption that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information within.
A.TIMESTAMP	OE.SYN_TIMESTAMP	The security objective counters this assumption because the TOE environment provides reliable, accurate and synchronized timestamps.
A.PHYSICAL_ENVIRONMENT	OE.SAFE_PHYSICAL_ENV	The security objective counters this assumption because the TOE and its environment shall be physically secure.
A.MALWARE	OE.ANTI_MALWARE	The security objective counters this assumption because the TOE platform shall be protected against Malware.
A.DDOS	OE.ANTI_DDOS	The security objective counters this assumption because the TOE platform and its network environment shall be protected against DDOS attacks.
A.THIRDPARTY	OE.THIRDPARTY	The security objective counters this assumption because the TOE only accepts all integrated third-party data transmitted to and from the TOE that are untempered and maintains integrity.

Table 13 shows the rationale for the Security Objectives and its assumptions

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

7 SECURITY FUNCTIONAL REQUIREMENTS (ASE_REQ.2)

This objective of this section is to determine whether the SFRs are clear, unambiguous and well-defined and whether it is internally consistent.

Class Family	Description	Dependencies
CLASS FIA: IDENTIFICATION AND AUTHENTICATION		
FIA_AFL: Authentication Failures		
FIA_AFL.1	Authentication failures handling	FIA_UAU.1 Timing of authentication
FIA_ATD: User Attribute Definition		
FIA_ATD.1	User attribute definition	No dependencies
FIA_SOS: Specification of Secrets		
FIA_SOS.1	Verification of secrets	No dependencies
FIA_UAU: User Authentication		
FIA_UAU.1	Timing of authentication	FIA_UID.1 Timing of identification
FIA_UAU.5	Multiple authentication mechanisms	No dependencies
FIA_UID: User Identification		
FIA_UID.1	Timing of identification	No dependencies
CLASS FAU: SECURITY AUDIT		
FAU_GEN: Security Audit Data Generation		
FAU_GEN.1	Audit data generation	FPT_STM.1 Reliable time stamps
FAU_GEN.2	User identity association	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
CLASS FTP: TRUSTED PATH/CHANNELS		
FTP_TRP: Trusted Path		
FTP_TRP.1	Trusted path	No dependencies
Class FDP: USER DATA PROTECTION		
FDP_ACC: Access Control Policy		
FDP_ACC.1	Subset access control	FDP_ACF.1 Security attribute role-based access control
FDP_ACF: Access Control Functions		
FDP_ACF.1	Security attribute-based access control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

Table 14 shows the Security Functional Requirements of the TOE

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

7.1 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

7.1.1 FIA_AFL: Authentication Failures

FIA_AFL.1 Authentication Failure Handling	
FIA_AFL.1.1	The TSF shall detect when [**five (5)**] unsuccessful authentication attempts occur related to [**user authentication during login**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [**surpassed**], the TSF shall [**lockout user account for a period of time, which is thirty (30) minutes**].
Application Note(s):	This requirement defines the action and behavior of user authentication process.

Table 15 shows FIA_AFL.1 Authentical Failures definition

7.1.2 FIA_ATD: User Attribute Definition

FIA_ATD.1 User Attribute Definition	
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**a) Authentication:** **i. User identity: User Name;** **ii. Passphrase: Password;** **iii. 2FA: User's OTP Secret;** **b) Authorization: Roles (privileges);** **c) User registration detail: Email address.**].
Application Note(s):	The User Name is a unique identifier used to identify each TOE user in the TOE. The Password consists of a series of rules which will be used together with the User Name security attribute to allow TOE user authentication. The Roles assigned to each TOE user will determine the functions he/she can access after he/she is logged in to the TOE. The Email address is used to receive email notifications from the MOzART team. The Two Factor Authentication (2FA) token will be used as an additional mechanism to identify the TOE user before he/she can gain access to the system. The 2FA token is generated using the Microsoft Authenticator App installed on the mobile device (supporting non-TOE software) registered in the TOE. The User's OTP Secret is the key stored inside the TOE and the registered mobile device used to generate the 2FA token. The User's OTP Secret will be used to validate the token entered into the system to check for its authenticity. The User's OTP Secret is installed onto the mobile device via the scanning of a QR code from Microsoft Authenticator generated by the TOE upon user first login to the TOE.

Table 16 shows FIA_ATD.1 User Attribute definition

7.1.3 FIA_SOS: Specification of Secrets

FIA_SOS.1 Verification of Secrets

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet: [**a) at least 8 characters;** **b) at least 1 uppercase character (A-Z);** **c) at least 1 lowercase character (a-z);** **d) at least 1 digit (0-9);** **e) at least 1 special character [<space>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~)] (extended ASCII codes are not allowed)**].
Application Note(s):	This requirement stipulates the rules of password complexity, strengthening user password during account creation and password reset process.

Table 17 shows FIA_SOS.1 Verification of Secrets definition

7.1.4 FIA_UAU: User Authentication

FIA_UAU.1 Timing of Authentication	
FIA_UAU.1.1	The TSF shall allow [**a) the account lockout interval feature after a series of unsuccessful login attempts (Identification and Authentication)** **b) the TOE to redirect/force the use of HTTPS communications channel when an insecure communications channel is used to access the TOE (Trusted Path/Channels)**] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Application Note(s):	The TOE will allow a maximum of five (5) attempts to be made by the unauthenticated TOE users to access the login portal before a lockdown period of 30 minutes is being imposed. During the lockdown period, no more login attempts can be made by the un-authenticated user. The 'Required SSL' setting in IIS server is turned on so that TOE users have to use HTTPS protocol to access the TOE. The use of HTTP to access the TOE is prohibited when 'Require SSL' option is turned on in IIS server.

Table 18 shows FIA_UAU.1 Timing of Authentication definition

FIA_UAU.5 Multiple Authentication Mechanisms	
FIA_UAU.5.1	The TSF shall provide [**Two Factor Authentication (2FA) after TOE user has correctly entered his/her User Name and password combination**] to support user authentication**.**
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [**6 digits numeric token (OTP) which will be generated by the Microsoft Authenticator (supporting non-TOE software) registered in the TOE user's mobile device (supporting non-TOE component) after the TOE user is authenticated via User Name and password. The token has a validity of 2 minutes; after which a new token needs to be regenerated. Once the token is being verified, the TOE user wil be brought to the home screen of the TOE**].
Application Note(s):	The 2FA token is generated using Microsoft Authenticator application (supporting non-TOE software) installed in the TOE user's registered mobile device.

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

Table 19 shows FIA_UAU.5 Multiple Authentication Mechanisms definition

7.1.5 FIA_UID: User Identification

FIA_UID.1 Timing of Identification	
FIA_UID.1.1	The TSF shall allow [**a) the account lockout interval feature after a series of unsuccessful login attempts (Identification and Authentication)** **b) the TOE to redirect/force the use of HTTPS communications channel when an insecure communications channel is used to access the TOE (Trusted Path/Channels)**] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Application Note(s):	The TOE will allow a maximum of five (5) attempts to be made by the unauthenticated TOE users to access the login portal before a lockdown period of 30 minutes is being imposed. During the lockdown period, no more login attempts can be made by the un-authenticated user. The 'Required SSL' setting in IIS server is turned on so that TOE users have to use HTTPS protocol to access the TOE. The use of HTTP to access the TOE is prohibited when 'Require SSL' option is turned on in IIS server. No form of identification is taken place when these functions mentioned above are executed.

Table 20 shows FIA_UID.1 Timing of Authentication definition

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

7.2 CLASS FAU: SECURITY AUDIT

7.2.1 FAU_GEN: Security Audit Data Generation

FAU_GEN.1 Audit Data Generation	
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) ~~Start-up and shutdown of the audit functions;~~ b) All auditable events for the [**detailed**] level of audit; and c) [**Other specifically defined auditable events are as follows:** **i) The start of TOE (MOzART CC) to indicate the starting of audit functions in the TOE. The start state of the TOE and the audit functions of the TOE are concurrent.** **ii) The shutdown of TOE (MOzART CC) to indicate the stopping of audit functions in the TOE. The stop state of the TOE and the audit functions of the TOE are concurrent.** **iii) User login attempts (regardless of successful or failed attempts) will be recorded. Information below will be logged in the audit trails:** **1.** User Name **2.** Timestamp **3.** Action (login/logout/request refresh token) **4.** Source URL **5.** Source IP **6.** Client ID **7.** User Name **8.** Login Type (user or app login) **9.** Status Code (result of the login attempt) **10.** Status Reason (info regarding the result of the login attempt, if any) **iv) All TOE user actions with regard to create, delete and update of data will be logged in the audit trails inside the TOE.**]
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**old and new values are being recorded in the audit trails**].
Application Note(s):	A **strikethrough** is conducted on a predefined SFR element when the component can be replaced with a better security feature or function present in the TOE. The **Start up and shutdown of the audit functions** is strikethrough because there is no startup or shutdown audit function in the TOE. The audit function automatically starts when the TOE Web Application is started and as soon as the TOE goes into operational state and stopped when the TOE Web Application is stopped. The TOE is able to audit/record when the startup and shutdown of the TOE Web Application happens via

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

	the Application_Start and Application_Shutdown built in functions in ASP.NET Global.asax. All auditable events based on the creation, deletion and update of the system configurations or data will be recorded by the TOE. Detailed auditable events are claimed as the TOE is capable of logging all fields that are being changed during the TOE's operational state.

Table 21 shows FAU_GEN.1 Audit Data Generation definition

FAU_GEN.2 User Identity Association	
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Application Note(s):	User Name is one of the mandatory fields that will be captured in the audit trails for the system to identify who has performed the action in the audit event. The User Name in the audit function cannot be empty or null.

Table 22 shows FAU_GEN.2 User Identity Association definition

7.3 CLASS FTP: TRUSTED PATH/CHANNELS

7.3.1 FTP_TRP: Trusted Path

FTP_TRP.1 Trusted Path	
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [**local**] 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 and disclosure**].
FTP_TRP.1.2	The TSF shall permit [**the TSF and local 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 other interactions between the local users and TOE**].
Application Note(s):	The TOE user is anyone who has access to the TOE via a web browser that has network link to the MOzART system.

Table 23 shows FTP_TRP.1 Trusted Path definition

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

7.4 CLASS FDP: USER DATA PROTECTION

7.4.1 FDP_ACC: Access Control Policy

<table>
<tr><th colspan="2">FDP_ACC.1 Subset Access Control</th></tr>
<tr><td>FDP_ACC.1.1</td><td>The TSF shall enforce the [Role-Based Access Control] on: [

Subjects:
a) authenticated and authorised users;

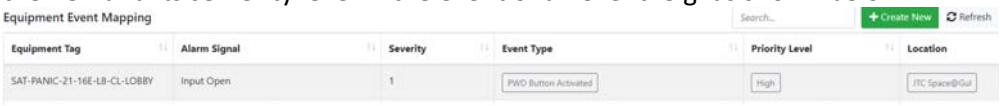
Objects:
a) Master data and system configuration data
b) Task data
c) Case data
d) User data

Operations:
a) Charts and Dashboard (View reports and manage dashboard)
b) Case Management (Manage cases and view incidents)
c) Task Management
d) Virtual Patrol (Perform virtual patrol)
e) Duty Roster (Manage duty roster)
f) Administrative Modules
g) CCTV Live View (View cameras)
h) Interactive 3D Maps (View maps)
i) Manage user profile and preferences
j) Change password
].</td></tr>
<tr><td>Application Note(s):</td><td>This requirement lists the subjects, objects and operations to be enforced based on the role-based access control matrix, correlated in the table below.

<table>
<tr><th rowspan="2">Objects</th><th colspan="10">Operations</th></tr>
<tr><th>(a)</th><th>(b)</th><th>(c)</th><th>(d)</th><th>(e)</th><th>(f)</th><th>(g)</th><th>(h)</th><th>(i)</th><th>(j)</th></tr>
<tr><td>Master data and system configuration data</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td></td></tr>
<tr><td>Task data</td><td>✓</td><td></td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Case data</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td></td><td>✓</td><td></td><td></td><td></td></tr>
<tr><td>User data</td><td>✓</td><td></td><td>✓</td><td></td><td>✓</td><td></td><td></td><td></td><td>✓</td><td>✓</td></tr>
</table>

The master data are referring to the data that need to be configure in the TOE before any users are to use the TOE efficiently.
o Case Type ➔ The type of cases that will be classified in the TOE. e.g. Incident, Serious Incident, Complaint, Enquiry, Event.
o SLA type ➔ the classification of SLA in the TOE. e.g. 1 hour, 1 minute, 2 minutes, etc.
o Reporting Channels ➔ the reporting channels where the case / incident is being reported. e.g. Email, Mobile App, Phone Call, SMS
o Case purpose ➔ The purpose classification to the case. e.g. Tenant, Certis Staff, FMC, Authorities, etc.
o Event Category ➔ The event categories that will be classified in the TOE. e.g. FM, Inactivity, Security, SOS</td></tr>
</table>

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

	o Event Types ➔ The event types that will be grouped under the event category. E.g. Accident on site, Acitve monitoring detection, Distress alert, etc. o Event Sources ➔ The sources of the event where it comes from. e.g. BMS, Camera, Intercom, VCA, etc. o Case Priority Types ➔ The classification of case priority in the TOE. e.g. Low, Medium, High. o Equipment Event Mapping ➔ The mapping of event type to an equipment in the TOE and its serverity level in the event of an event. e.g. as shown below  o Task Type ➔ The type of tasks being assigned in the TOE. e.g. Security Task o Task Template ➔ The task template defines the steps that need to be performed during an Event. o Sites ➔ The site aka building where the TOE will be operated on. o Floors ➔ The floor definition in a building o Locations ➔The location where the building is located o Cameras ➔ The equipment configuration in the TOE that will be used for CCTV monitoring o Guard Tour ➔ The configuration of a pre-defined checkpoints and path where the security staff need to perform in a stipulated duration. o Virtual Patrol ➔ The configuration of a virtual patrol task where user can define the duration of the monitoring and the cameras involved in the virtual patrolling. o Duty Roster Types ➔ The duty type definition and its duration for a specific roster. o Teams ➔ The name of the group where the staff will be grouped under. o Staff ➔ The staff info that will work in the site(s) where the TOE is operating o Audit reporting ➔ The audit trails data that capture user activities within the TOE. The **case data** consists of the following information: • Case ID • Short description of the case • Equipment/Asset related to the case • Event Type • Location of the event • Time stamp of the event • Severity of the event • Priority of the event • Critical flag • SLA tie to the case • Case reference number • False alarm indicator • Reporting channel (if applicable) • Event created by • Event created timestamp • Event modified by • Event modified timestamp • Event assigned to which staff (if applicable) • Event assigned by which staff (if applicable) • Event Status

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

	• Task templates assigned to the event • Reason assigned to the case (if applicable) • Purpose assigned to the case (if applicable) • Case resolved timestamp • Case reopened timestamp (if applicable) • Camera ID that captures the event (if applicable) The **task data** consists of the following information: • Task name • Task description • Task long description • Task type • Case ID • Case reference number • Task status • Task created by • Task created timestamp • Task modified by • Task modified timestamp • Task instruction • SLA tie to the case • Task Progress • Staff assigned to handle the task • Team assigned to handle the task The **user data** consists of the following information: • User Name • Password • User Preferences • Email • Mobile Number • Staff ID

Table 24 shows FDP_ACC.1 Subset Access Control definition

7.4.2 FDP_ACF: Access Control Functions

FDP_ACF.1 Security Attribute Based Access Control	
FDP_ACF.1.1	The TSF shall enforce the [**Role-Based Access Control**] on: [**Subjects:** **a) authenticated and authorised users;** **Objects:** **a) User data** **Security Attributes:** **a) Roles**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

	a) The roles granted is tied to the function where the TOE user can access. **b) The roles are correct in accessing all designated functions.** **c) roles are correct during access to Charts and Dashboard (View reports and manage dashboard)** **b) roles are correct during access to Case Management (Manage cases and view incidents)** **c) roles are correct during access to Task Management** **d) roles are correct during access to Virtual Patrol (Perform virtual patrol)** **e) roles are correct during access to Duty Roster (Manage duty roster)** **f) roles are correct during access to Administrative Modules** **g) roles are correct during access to CCTV Live View (View cameras)** **h) roles are correct during access to Interactive 3D Maps (View maps)** **i) roles are correct during access to Manage user profile and preferences** **j) roles are correct during access to Change password**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].
Application Note(s):	1) This requirement lists the subjects, objects and security attributes to be enforced based on the role-based access control matrix. 2) This requirement also defines the behavior and rule for operations between controlled subjects and controlled objects. 3) If the user's access control matrix does not contain the said function; the user will not be able to acces the function. 4) The following rules mentioned in FDP_ACF.1.2 projects a security flow for access controls maintained after the authentication of the TOE users. All TOE users will require authentication from the TOE through the matching security attributes User name and password before they are authorized to perform their permitted actions.

Table 25 shows FDP_ACF.1 Security Attribute Based Access Control definition

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

7.5 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

7.5.1 Rationale for SFR Mapped to Security Objectives

Security Objective	SFR	Rationale
O.SEC_ACCESS	FIA_ATD.1	This SFR will maintain a list of security attributes belonging to individual users in order to uniquely identify them.
	FIA_UID.1	This SFR will ensure that the person being granted access is a legitimate user, and that the assignation of user roles and access controls must be met before user is permitted to the required TOE functions.
	FDP_ACC.1	This SFR will ensure the access to TOE operations are based on the roles assigned and only minimal and/or specific permissions are granted to the user.
	FDP_ACF.1	This SFR will ensure the access to TOE data and functions is restricted to the owner of data or authorized users to a respective function.
	FAU_GEN.1	This SFR will ensure all critical changes to the system are recorded and traceable to the user who performed the action.
	FAU_GEN.2	This SFR will include the user's unique identifier (User Name) on the audit log.
O.SEC_AUTHENTICATE	FIA_AFL.1	This SFR will increase the difficulty of automated brute force and DOS attacks by locking the user account for 30 minutes if the continuous failure attempt is more than 5 times.
	FIA_SOS.1	This SFR will ensure user's password complexity is met.
	FIA_UAU.1	This SFR will ensure that the assignment of User Name and password combination must be met before user is authenticated.
	FIA_UAU.5	This SFR will ensure that the authentication process requires a multi-level verification before user is authenticated.
	FAU_GEN.1	This SFR will ensure all critical changes to the system are recorded and traceable to the user who performed the action.
	FAU_GEN.2	This SFR will include the user's unique identifier (User Name) on the audit log.
O.SEC_COMMUNICATION	FTP_TRP.1	This SFR provides secured and encrypted communication for data transfer from and to the TOE.

Table 26 shows the Rationale for SFR Mapped to Security Objectives

7.5.2 SFR Dependency Rationale

Class Family	Dependency	Dependency Satisfied	Justification
FIA_AFL.1	FIA_UAU.1	Yes	-
FIA_ATD.1	No dependencies	-	-
FIA_SOS.1	No dependencies	-	-
FIA_UAU.1	FIA_UID.1	Yes	-
FIA_UAU.5	No dependencies	-	-

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

FIA_UID.1	No dependencies		
FAU_GEN.1	FPT_STM.1	No	TOE's operational environment shall provide reliable timestamps to the TOE.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes	-
FTP_TRP.1	No dependencies	-	-
FDP_ACC.1	FDP_ACF.1	Yes	-
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	No	TOE's operational environment shall provide all relevant static attributes used for account access control management to the TOE.

Table 27 shows the SFR Dependency Rationale

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

8 SECURITY ASSURANCE REQUIREMENTS (ASE_REQ.2)

This ST implements the Security Assurance Requirements (SARs) of the Evaluation Assurance Level 2 (EAL2) package. The assurance components are summarized in the following table which is drawn from CC Part 3:

Assurance Class	Assurance Component	Details	Rationale
Development	ADV_ARC.1	Security architecture description	To conform to the EAL2 requirement
	ADV_FSP.2	Security-enforcing functional specification	A mandatory document to sign off for the customer during a SDLC and also to conform to the EAL2 requirement
	ADV_TDS.1	TOE design (Basic design)	To conform to the EAL2 requirement
Guidance Documents	AGD_OPE.1	Operational user guidance	To conform to the EAL2 requirement
	AGD_PRE.1	Preparative procedures	A installation guide for the
Life-cycle Support	ALC_CMC.2	CM capabilities (Use of a Configuration Management system)	To conform to the EAL2 requirement
	ALC_CMS.2	CM scope (Parts of the TOE Configuration Management coverage)	To conform to the EAL2 requirement
	ALC_DEL.1	Delivery procedures	To conform to the EAL2 requirement
Security Target Evaluation	ASE_CCL.1	Conformance claims	To conform to the EAL2 requirement
	ASE_ECD.1	Extended components definition	To conform to the EAL2 requirement
	ASE_INT.1	ST introduction	To conform to the EAL2 requirement
	ASE_OBJ.2	Security objectives	To conform to the EAL2 requirement
	ASE_REQ.2	Derived security requirements	To conform to the EAL2 requirement
	ASE_SPD.1	Security problem definition	To conform to the EAL2 requirement
	ASE_TSS.1	TOE summary specification	To conform to the EAL2 requirement
Tests	ATE_COV.1	Coverage (Evidence of coverage)	To conform to the EAL2 requirement
	ATE_FUN.1	Functional testing	A requirement document and process during the SDLC for user to sign off and accept the system. Also to conform to the EAL2 requirement
	ATE_IND.2	Independent testing – sample	A required process and report for user to accept

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

			the system and also to conform to the EAL2 requirement
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis	A required process and report for user to accept the system and also to conform to the EAL2 requirement

Table 28 shows the mapping of assurance components and its assurance class

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

9 TOE SUMMARY SPECIFICATION (ASE_TSS.1)

This section specifies the security functional requirements addressed by the TOE.

9.1 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:

- Security Audit;
- Identification and Authentication;
- Trusted Path/Channels; and
- User Data Protection.

9.2 SECURITY AUDIT

Audit logs are generated by the TOE with the association of the TOE user and the event. The audit level of the TOE is set to full, which indicates all possible auditable events logged when a TOE user performs any operation within the TOE. Actions such as create, update and delete are logged inside the audit trails.

The auditable events that will be logged by the TOE are as below; the audit trails can only be viewed by Administrator and Supervisor; no changes can be made to the audit trails by any user roles:

i. The starting and stopping of TOE
ii. User authentication process, i.e. the TOE's security audit trail records the login attempts of a TOE user
iii. All TOE user actions inside the TOE such as:
    a. Create record
    b. Delete record
    c. Update record

The values that will be captured in the security audit are:

a. User Name - this user security attribute is recorded in audit trails to show the action(s) taken by the responsible individual(s)
b. User actions – Create, delete and update objects or records
c. User action date and time
d. Original values - values before modification
e. New values - values after modification

During the authentication process, the audit trails will capture the user login attempts to the TOE regardless success or failure. The user name, timestamp and the status of the authentication will be captured in the audit logs.

All the user actions involving create, delete and update of records will be captured by the audit logs. The user name, timestamp, user action, the value changed by the user (old vs new) will be logged in the audit logs.

FAU_GEN.1 ➔ All user actions that are pertaining to data changes (create/delete/update) will be subjected to an auditable event that will be logged by the TOE when the action is successfully persisted in the database. With the exception of user login where unsuccessful login attempts will also be logged. Actions such as function access (e.g. report generation), unauthorized function access (e.g. Operator tries to access audit trail report where he/she doesn't have the user rights) will not be logged as it does not avocate to any data changes in the TOE. The audit trails cannot be bypassed nor shutdown by any user or any means if the TOE is in its operating state. The audit

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

trails start functioning immediately when the TOE is in its operating state and will only stop working if and only if the TOE is not in its operating state.

FAU_GEN.2 ➔ Once an auditable event is being captured by the TOE; the action type (create/delete/update), time stamp of the action, user who performs the action, result of the action (success/fail) plus the changes made (old vs new value) will be recorded in the audit trails by the TOE audit function.

Security Functional Requirements Satisfied:

- FAU_GEN.1
- FAU_GEN.2

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

9.3 IDENTIFICATION AND AUTHENTICATION

TOE provides user interfaces which allow administrator to manage the TOE's security attributes. The user interface provides web-based access to TOE functions through web browsers. The user interface module enforces identification and authentication mechanism before any TOE user can perform any actions on the TOE.

TOE users are required to set their password according to a defined password requirement, where the minimum characters are set to eight (8) characters, and fulfil the following:

i. at least 1 uppercase character (A-Z);
ii. at least 1 lowercase character (a-z);
iii. at least 1 digit (0-9);
iv. at least 1 special character [<space>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~)] (extended ASCII codes are not allowed)

If the TOE user fails to abide to the password requirements; the TOE will prompt an error message asking the TOE user to create a password fulfilling the above criteria.

The following TOE Security Functions will act on behalf of the TOE user before he/she is authenticated and identified:

- A trusted and secure communications path will be established between the TOE and the TOE users. (Trusted Paths/Channels)
- The account lockout interval feature will be executed after a series of unsuccessful login attempts are detected on a TOE user. (Identification and Authentication)

The authentication attempts are monitored and controlled by the TOE, where the account will be locked out for thirty (30) minutes after five (5) invalid attempts.

The TOE maintains the following list of security attributes belonging to individual users:

i. User Name
    a. The User Name is a unique identifier used to identify each TOE user in the TOE.
ii. Password
    a. The Password consists of a series of rules which will be used together with the User Name security attribute to allow TOE user authentication.
iii. Roles
    a. The Roles assigned to each TOE user will determine the functions he/she can access after he/she is logged in to the TOE.
iv. Email address
    a. The Email address is used to receive email notifications from the MOzART team.
v. User's OTP Secret.
    a. The Two Factor Authentication (2FA) token will be used as an additional mechanism to identify the TOE user before he/she can gain access to the system. The 2FA token is generated using the Microsoft Authenticator App installed on the mobile device (supporting non-TOE software) registered in the TOE. The User's OTP Secret is the key stored inside the TOE and the registered mobile device used to generate the 2FA token. The User's OTP Secret will be used to validate the token entered into the system to check for its authenticity.
    b. The User's OTP Secret is installed onto the mobile device via the scanning of a QR code from Microsoft Authenticator generated by the TOE upon user first login to the TOE.

During the first successful login process, the TOE user will be instructed to download the 2FA software from the AppStore or PlayStore. The TOE will display a QR code for TOE user, TOE user will then scan the QR code into the 2FA mobile application. The 2FA mobile application will then register MOzART into its registry.

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

Upon subsequent TOE user authentication to the TOE, the TOE user will need to enter the OTP shown on the 2FA mobile application to complete the authentication process.

FIA_AFL.1 ➔ The TOE keeps tracks of number of failed authentication attempt of the user. If a user exceeds the predefined authentication attempt threshold (5) the TOE will lock the user from trying to login again for 30 minutes. This prevents unauthorized user from attempting a brute force attack to the TOE.

FIA_ATD.1 ➔ The TOE is using the following attributes in identifying a TOE user during authentication process. The TOE user's user name, password and 2FA token after the user name and password authentication passes in the TOE login page. Once the user is authenticated, his/her access is binded to the role(s) that has been assigned to him/her during the account creation. In addition to that the user's email address is used to receive email notification from the TOE.

FIA_SOS.1 ➔ The TOE enforces a password policy where the TOE user has to abide to a set of password complexity set by the TOE when choosing his/her password. If the user fails to fulfil the password complexity requirement, the TOE will reject the password enter and prompt the user to re-enter his/her password. The TOE checks for this password complexity requirement during the user authentication process and change user password function when the user wants to change his/her password.

FIA_UAU.1 ➔ Before the user is authenticated, the TOE keeps track of failed login attempts and lock the user out for 30 minutes if 5 failed login attemtps were recorded by the user. The TOE also enforces the use of HTTPS protocol when user tries to access it and redirect the use of HTTPS protocol when a HTTP protocol is used to access the TOE. Last but not least the TOE will ensure all user accessing the TOE are authenticated before he/she can access any function.

FIA_UAU.5 ➔ The TOE implements two factor authentication on the users who have successfully authenticated themselves using the user name and password at the TOE login page. The 2FA acts as a second level of security to ensure the users who have managed to login via the TOE login page is indeed the TOE users themselves as the 2FA token can only be generated and verified via the TOE user's registered mobile device.

FIA_UID.1 ➔ Before the user is identified, the TOE keeps track of failed login attempts and lock the user out for 30 minutes if 5 failed login attemtps were recorded by the user. The TOE also enforces the use of HTTPS protocol when user tries to access it and redirect the use of HTTPS protocol when a HTTP protocol is used to access the TOE. Last but not least the TOE will ensure all user accessing the TOE are identified before he/she can access any function.

Security Functional Requirements Satisfied:

- FIA_AFL.1
- FIA_ATD.1
- FIA_SOS.1
- FIA_UAU.1
- FIA_UAU.5
- FIA_UID.1

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

9.4 TRUSTED PATH/CHANNELS

The TOE is hosted on a web server installed with the use of secure communication protocol TLS 1.2 and above. The communication channel between the TOE and its local TOE users is enforced with the use of HTTPS, where data traffic to and fro the TOE users are encrypted and protected against data or information being modified or disclosed. In addition to that, the TOE will not establish a connection with the client if the TOE is accessed via HTTP.

The TOE is hosted on a web server installed with the use of secure communication protocol TLS 1.2 and above. The secure communication prototcol is set by applying a TLS 1.2 and above, together with a trusted and legitimate certificate onto the URL in the Internet Information Services (IIS) web server where the TOE is being hosted. The certificate will be purchased by the TOE users themselves from a trusted certificate authority.

The communication channel between the TOE and its local TOE users is enforced with the use of HTTPS by enforcing the use of SSL in the IIS settings, where data traffic to and fro the TOE users are encrypted and protected against data or information being modified or disclosed during data transmission.

All modules, operations and tasks in the TOE require the trusted path to be established before TOE users can access it. In addition to that, the TOE will not establish a redirection with the TOE users if the TOE is accessed via HTTP, forcing the TOE users to access the TOE via HTTPS protocol.

The trusted path between the TOE and its users is established by installing a TLS 1.2 and above certificate onto the web browser where TOE is being hosted. The web server is being configured such that only HTTPS protocol is allowed to be used when TOE is being accessed. If the web browser detects a HTTP protocol in the URL, it will redirect the browser to use HTTPS protocol to ensure the communication channel is always secured between the TOE and the browser that's accessing it.

FTP_TRP.1 ➔ HTTPS protocol is a must for the TOE users to access the TOE via a browser. The TOE will not establish a connection with any web browsers if the protocol used to access the TOE is not in HTTPS. The TOE will auto route the user to use HTTPS protocol to access the TOE if the web server detects a HTTP protocol. This prevents any users from trying to access the TOE via an unsecured channel where the data will be transmitted in clear between the TOE and the TOE users.

Security Functional Requirements Satisfied:

- FTP_TRP.1

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

9.5 USER DATA PROTECTION

The users of the TOE are assigned with Role-Based Access Control during account creation. The Role-based Access Control denotes the functions/actions which the TOE user can access to after he/she is successfully authenticated by the TOE. Only the authenticated and authorized TOE users with the necessary roles can access the functions that are defined in the access matrix below.

Role	Modules				
	Case Management	Virtual Patrol	Duty Roster	System Administration	User Profile Management
Administrator	✓	✓	✓	✓	✓
Supervisor	✓	✓	✓		✓
Operator	✓	✓			✓

Table 29 shows the mapping of roles and the modules that it can access to

The functions within each module is listed as follows.

Module	Functions	Description
Case Management	• Case classification/monitoring • Task assignment/dispatch • Report generation	These functions are used by TOE users who are assigned the Operator role to manage and monitor the security operations. This module can also be utilized by the Administrator and Supervisor roles to only perform case escalation, task assignments, reporting.
Virtual Patrol	• CCTV Monitoring • Report generation • Incident reporting	Used by TOE users with Operator role to monitor pre-configured site areas via CCTV. This module can also be utilized by the all other TOE user roles to perform the same functions as the Operator.
Duty Roster Management	• Manage staff availability • Manage duty plans • Assign tasks to staff	Used by TOE users with Administrator/Supervisor role manage work and assignment orders. The administrator and supervisor create duty rosters for the operator to perform task scheduling.
System Administration	• Create, modify master records o Case Type o SLA type o Reporting Channels o Case purpose o Event Category o Event Types o Event Sources o Case Priority Types o Equipment Event Mapping o Task Type	This module allows Administrators to adjust TOE system configurations and master data.

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888

	o Task Template o Sites o Floors o Locations o Cameras o Guard Tour o Virtual Patrol o Duty Roster Types o Teams o Staff o Audit reporting	
User Profile Management	• Update preferences • Change password	This module allows TOE users to change their own personal information, personal default settings, and account password.

Table 30 shows the functions in each module within the TOE

Whenever a TOE function is being accessed by the user, the TOE will verify the user is authorized and authenticated and the user role that the user has been assigned has the necessary rights to access the function.

FDP_ACC.1 ➔ The access of the TOE is governed by the Role-Based Access Control mechanism where users are assigned with a set of roles with user rights tied to the role(s) during his/her account creation. The access of the user is strictly checked against the role(s) that's being assigned to them to see if he/she has the necessary rights to the function when he/she tries to access it.

FDP_ACF.1 ➔ The TOE verifies if the authenticated user has the role and sufficient rights to access the function, he/she wants to access in the TOE before granting the user the access to the function that he/she chooses. If the user does not possess the required role/access the TOE will deny the user from access the said function.

Security Functional Requirements Satisfied:

- FDP_ACC.1
- FDP_ACF.1

[End of Document]

Certis CISCO Security Pte Ltd @ 20 Jln Afifi, Certis CISCO Centre, Singapore 409179.
Tel: +65 – 6747 2888