MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

C117 Certification Report

MOzART Command Center Web Portal v1.1

File name: ISCB-5-RPT-C117-CR-v1
Version: v1
Date of document: 26 July 2021
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)

T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

Securing Our Cyberspace

C117 Certification Report

MOzART Command Center Web Portal v1.1

26 July 2021

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C117 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C117-CR-v1
ISSUE:	v1
DATE:	26 July 2021
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (726630-U)

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 26 July 2021, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	11 June 2021	All	Initial draft
V1	26 July 2021	Page xii, Page vi, Page 2, Para 44, 54 & 55	1. Update on TÜV name 2. Add Organizational Security Policy table 3. Update date of certification

Executive Summary

The Target of Evaluation (TOE) is web-based application portal called 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.

The scope of the evaluation is defined by the Security Target (Ref[6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by TÜV Austria CyberSecurity Lab Sdn. Bhd (TACSL) and the evaluation was completed on 11 June 2021. The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that MOzART Command Center Web Portal (MOzART CC) v 1.1 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 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).

2 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.

3 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.

4 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.

5 The MOzART CC is a highly sophisticated Command Center, acting as the 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.

1.2 TOE Identification

6 The details of the TOE are identified in Table 1: TOE Identification below.

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C117
TOE Name	MOzART Command Center Web Portal
TOE Version	V1.1
Security Target Title	MOzART Command Center Web Portal
Security Target Version	V1.26
Security Target Date	11 May 2021
Assurance Level	Evaluation Assurance Level 2

Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 2
Sponsor	Certis CISCO Security Pte Ltd (Certis) 20, Jalan Afifi, Singapore 409179
Developer	Certis CISCO Security Pte Ltd (Certis) 20, Jalan Afifi, Singapore 409179
Evaluation Facility	TÜV Austria CyberSecurity Lab Sdn. Bhd (TACSL)

1.3 Security Policy

7 In Table 2 below shows details of Organizational Security Policy

Table 2: Organizational Security Policy

<table>
<tr><th>OSP Identifier</th><th>OSP Statement</th></tr>
<tr><td>P.PASSWORD</td><td>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.</td></tr>
<tr><td>P.ACCESS_ROLE</td><td>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.</td></tr>
</table>

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.

1.4 TOE Architecture

8 The TOE consist of logical and physical boundaries which are described in Section 1.6 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

9 The logical boundary of the TOE is summarized below:

- Identification and Authentication
    - 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 TOE are as below:
        - The starting and stopping of TOE
        - User authentication process, i.e. the TOE’s security audit trail records the login attempts of a TOE user
        - 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.

1.4.2 Physical Boundaries

10 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).

11 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.

12 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.

13 The 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.

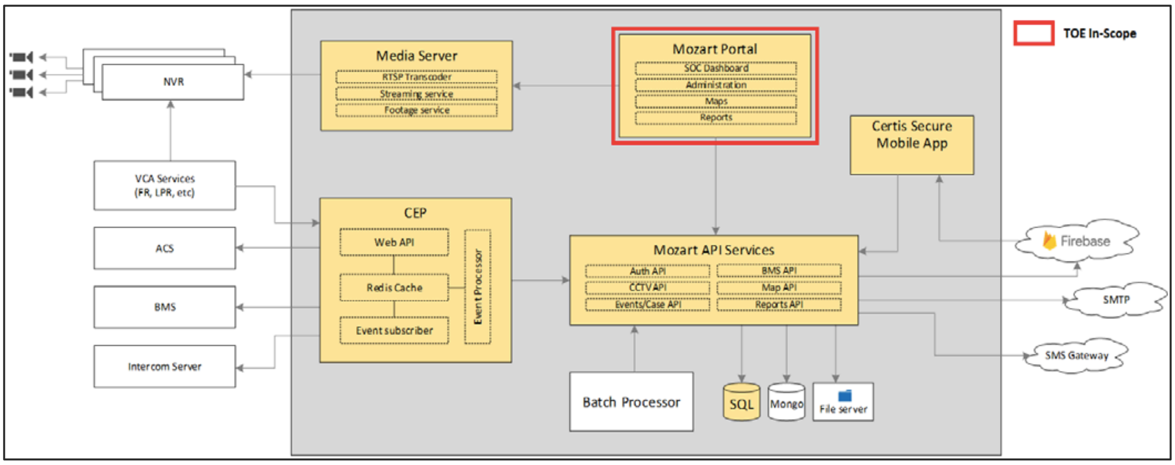

Figure 1: MOzART system architecture, with physical scope of the TOE, MOzART Command Center Web Portal boxed in red.

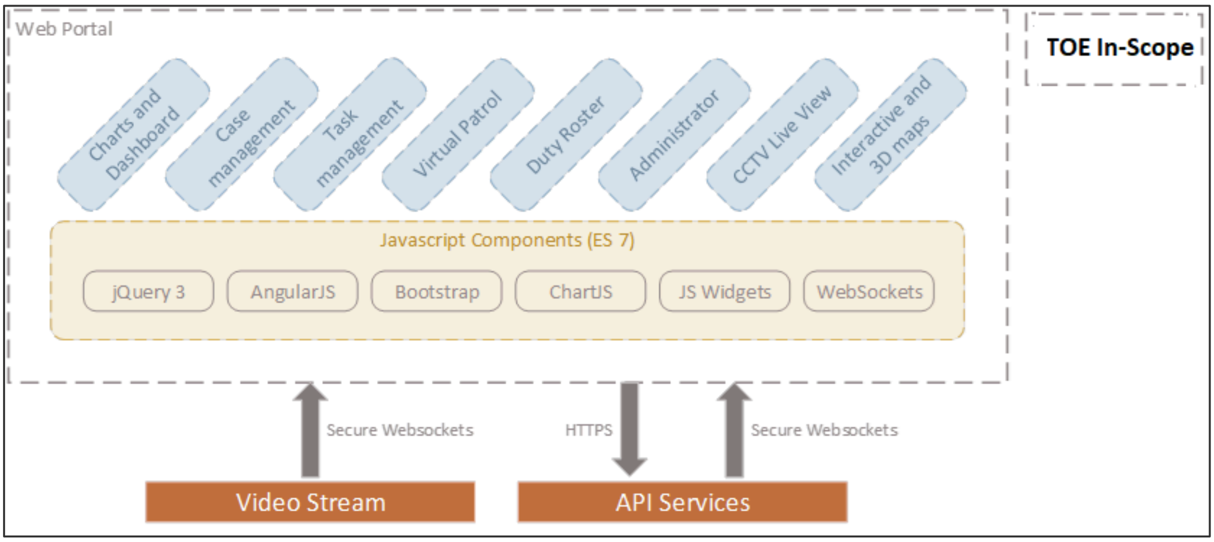

Figure 2: Detailed application architecture together with the physical scope of TOE boxed in dotted-lines.

14 The TOE in scope provides the access and usage of the MOzART CC modules and functions directly.

15 The TOE's main usage provides TOE users of monitoring, operating, managing and administering physical security incidents.

16 The target audience of the ST encompasses consumers who are interested in maintaining and controlling physical security.

17 The MOzART CC allows consumers to have "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.

18 The TOE can only be used by authenticated users via web browser.

1.5 Clarification of Scope

19 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

20 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

21 Potential consumers of the TOE are advised that some functions and services of the overall product have not have been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

22 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand the requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Environmental assumptions

23 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 3: Assumptions for the TOE Environment

Environment	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.

1.7 Evaluated Configuration

24 This section describes the configurations of the TOE that are included within the scope of the evaluation. The evaluated configuration for TOE is 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).

25 In Figure 1 Section 1.4.2 detailed architecture that shows the relationship between the TOE and supporting non-TOE components of the MOzART platform .

26 In Figure 2 Section 1.4.2 drills down into the software architecture of the TOE, with the different subsystems identified. Even though the Javascript Components (ES 7) is packaged together with the TOE, it is not within the scope this evaluation.

27 The TSF subsystems are chosen as they form the core functionalities of MOzART CC; the TOE works in tandem when the TSF subsystems function according to its designated functionalities.

28 The subsystems listed below can be access without authentication:

- User login

29 The subsystems listed below can be access only after authentication:

- User profile
- Charts & Dashboard
- Case Management
- Task Management

- CCTV Live View
- Interactive 3D Maps
- Virtual Patrol
- Duty Roster
- System Administration

1.8 Delivery Procedures

30 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

31 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 TOE Delivery Procedures

32 a) Delivery of TOE and Non-TOE Components Packaging

The TOE and supporting non-TOE components required during the onsite installation will be copied into a secured hard drive which later be delivered by Certis Logistics Team to the designated TOE user's premises where the installation will take place:

The secured hard drive that contains the installation kit and necessary components for installation is protected with password. The contents inside the secured hard drive is encrypted and not visible unless a valid password has been used to unlock the contents inside it. The password used to unlock the secured hard drive is sent via email to the TOE user. The TOE user will then need to unlock the contents of the secured hard drive for the Certis Deployment Team to begin their necessary tasks.

The installation kit will be prepared by Certis Deployment Team; once ready, the secured hard drive will be given to the MOzART License Control Team to secure the hard drive will a password. This prevents the Certis Deployment Team from accessing the contents inside the secured hard drive before having the authorized TOE user to unlock the hard drive contents via emailed password.

The secured hard drive will be placed inside a plastic container and secured with tamper-proof stickers and later kept inside a tamper-proof bag by the MOzART License Control Team before being delivered to the TOE user's premises for installation by the

Certis Logistics Team. The tamper-proof bag's code will be torn off from the tamper-proof bag and kept by Certis Deployment Team as a reference copy.

All supporting non-TOE hardware required by the TOE and supporting non-TOE software would have been delivered onsite by the Certis Logistics Team prior to the arrival of the secured hard drive and Certis Deployment Team. The supporting non-TOE hardware required will be mounted inside the racks and ready for installation. The secured hard drive will be shipped using a tamper proof bag and all the supporting non-TOE hardware will be pasted with tamper-proof stickers onto its containers before they are shipped out to prevent it from being opened by unauthorized personnel.

33 b) Delivery of TOE and Non-TOE Components Packaging for Overseas Customers

The TOE and supporting non-TOE components required during the onsite installation will be copied into a secured hard drive which will later be delivered by to the designated TOE user's premises where the installation will take place.

The secured hard drive that contains the installation kit and necessary components for installation is protected with password. The contents inside the secured hard drive is encrypted and not visible unless a valid password has been used to unlock the contents inside it. The password used to unlock the secured hard drive is sent via email to the TOE user. The TOE user will then need to unlock the contents of the secured hard drive for the Certis Deployment Team to begin their necessary tasks.

The installation kit will be prepared by Certis Deployment Team; once ready, the secured hard drive will be given to the MOzART License Control Team to secure the hard drive will a password. This prevents the Certis Deployment Team from accessing the contents inside the secured hard drive before having the authorized TOE user to unlock the hard drive contents via emailed password.

The secured hard drive will be kept inside a tamper-proof bag by the MOzART License Control Team before being delivered to the TOE user's premises for installation by designated logistics company such as DHL, Fedex, UPS or any courier services that provides online package tracking facility.

All supporting non-TOE hardware required by the TOE and supporting non-TOE software would have been delivered onsite by the chosen logistics company prior to the arrival of the secured hard drive and Certis Deployment Team. The supporting non-TOE hardware required will be mounted inside the racks and ready for installation. The secured hard drive will be shipped using a tamper proof bag and all the supporting non-TOE hardware will be pasted tamper-proof stickers before they are shipped out to prevent it from being opened by unauthorized personnel.

In addition to the existing tamper proof bag and stickers to safe keep the secured hard drive and supporting non-TOE hardware; the packaging boxes that house these items will be sealed with tamperproof stickers to prevent the boxes from being opened before it reaches the TOE user's premises.

2 Evaluation

34 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

35 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

36 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

37 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

38 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

39 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

40 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

41 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

42 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

43 The evaluators confirmed that the TOE guidance was fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

44 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by TÜV Austria CyberSecurity Lab Sdn. Bhd (TACSL). The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.4.1 Assessment of Developer Tests

45 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators tests are consistent with the developers test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

46 At EAL 2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation,

examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

47 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 4: Independent Functional Test

Test ID	Description	Security Function	Results
Test-ATE-001	**Secure Channel Test (HTTPS)** TOE users need to verify the presence of the padlock icon (found beside the URL) within the web browser. This indicates the connection is identified by the web browser as legitimate certificate issued and signed by a Certificate Authority.	FTP_TRP.1	Passed
Test-ATE-002	**Secure Channel Test (HTTP)** TOE user will be redirected to the TOE via HTTPS protocol. TOE users need to verify the presence of the padlock icon (found beside the URL) within the web browser. This indicates the connection is identified by the web browser as legitimate certificate issued and signed by a Certificate Authority.	FTP_TRP.1	Passed

Test ID	Description	Security Function	Results
Test-ATE-003	**User Login (Administrator) Test** The TOE user should be redirected to the TOE Mode Selection Page.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_UAU.1 FIA_UAU.5 FIA_UID.1	Passed
Test-ATE-004	**Change Password (Administrator) Test** The user new password is being updated to the system when “Submit” is clicked. User is able to login to the TOE using the new password.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FIA_ATD.1 FIA_SOS.1	Passed
Test-ATE-005	**Change Password (Administrator) Test – Old password mismatch** System prompts “Incorrect password’ when “ Submit” is clicked.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FIA_ATD.1 FIA_SOS.1	Passed
Test-ATE-006	**User Profile Management Test** The user profile / user preference should be updated in the system.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FIA_ATD.1 FIA_SOS.1	Passed
Test-ATE-007	**Create Building Test** The Building will be created and reflected in the Buildings listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed

Test ID	Description	Security Function	Results
Test-ATE-008	**Update Floor Test** The Floor will be updated and reflected in the selected Building listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-009	**Create Case Type Test** The case type will be created and reflected in the case type listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-010	**Update SLA Configurations Test** The SLA configuration will be updated and reflected in the SLA configuration listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-011	**Create Purposes Test** The Purpose will be created and reflected in the Purpose listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-012	**Update Event Categories Test** The Event Category will be updated and reflected in the Event Category listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-013	**Create Case Priority Types Test** The Priority Level will be created and reflected in the Priority Level listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed

Test ID	Description	Security Function	Results
Test-ATE-014	**Update Task Type Test** The Task Type will be updated and reflected in the Task Type listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-015	**Create Cameras (Equipment Management) Test** The camera (equipment) will be created and reflected in the Equipment Management listing for the selected location.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-016	**Update Equipment Event Mapping Test** The Equipment Event Mapping will be updated and reflected in the Equipment-Event Mapping listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-017	**Create Teams Test** The Team will be created and reflected in the Teams listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-018	**Update Guard Tour Test** The Guard Tour will be updated and reflected in the selected Guard Tour listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-019	**Create Duty Roster Types Test** The Duty Type will be created and reflected in the Duty Type listing.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed

Test ID	Description	Security Function	Results
Test-ATE-020	**Create Duty Roster – _Staff Availability Test** The staff availability is highlighted on the calendar.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-021	**Create Duty Roster – Duty Plan Test** The newly created Duty Plan is shown in the Duty Plan list.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-022	**Create Duty Roster – Work Schedule Test** The Work Schedule is highlighted on the calendar.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-023	**Audit Reporting Test** The audit trails are shown based on the selection criteria.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2	Passed
Test-ATE-024	**User Login – Failed Attempts (Supervisor) Test** The TOE user should be locked from login to the TOE for thirty (30) minutes after five (5) invalid login attempts.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_UAU.1 FIA_UAU.5 FIA_UID.1	Passed
Test-ATE-025	**Change Password (Supervisor) Test – New and confirm password mismatch** System prompts “Your new password do not match” when “Submit” is clicked.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FIA_ATD.1 FIA_SOS.1	Passed

Test ID	Description	Security Function	Results
Test-ATE-026	**User Profile Management Test** The user profile / user preference should be updated in the system.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FIA_ATD.1 FIA_SOS.1	Passed
Test-ATE-027	**Update Duty Roster - Staff Availability Test** The updated staff availability is highlighted on the calendar.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-028	**Update Duty Roster – Duty Plan Test** The updated Duty Plan is shown in the Duty Plan list.	FTP_TRP.1 FAU_GEN.1 FAU_GEN.2 FDP_ACC.1 FDP_ACF.1	Passed
Test-ATE-029	**Update Duty Roster – Work Schedule Test** The Work Schedule is highlighted on the calendar.	FTP_TRP.1, FAU_GEN.1, FAU_GEN.2, FDP_ACC.1, FDP_ACF.1	Passed
Test-ATE-030	**View Incidents Test** The selected incident / event will be shown in a new tab in the TOE Main Page.	FTP_TRP.1, FAU_GEN.1, FAU_GEN.2, FDP_ACC.1, FDP_ACF.1	Passed
Test-ATE-031	**Create Case Test** The TOE Main Page will be refreshed, and the list of existing incidents/cases will be displayed, along with the newly created incident/case.	FTP_TRP.1, FAU_GEN.1, FAU_GEN.2, FDP_ACC.1, FDP_ACF.1	Passed

Test ID	Description	Security Function	Results
Test-ATE-032	**Create Task Test** The task will be created in the case.	FTP_TRP.1, FAU_GEN.1, FAU_GEN.2, FDP_ACC.1, FDP_ACF.1	Passed
Test-ATE-033	**User Login – Invalid 2FA Token (Operator) Test** The TOE user will not be able to gain access to the TOE without entering a valid 2FA token.	FTP_TRP.1, FAU_GEN.1, FAU_GEN.2, FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1	Passed
Test-ATE-034	**Change Password (Operator) Test – Password does not meet the defined complexity** System prompts “Your new password does not meet the required password strength” when “Submit” is clicked	FTP_TRP.1, FAU_GEN.1, FAU_GEN.2, FIA_ATD.1, FIA_SOS.1	Passed
Test-ATE-035	**User Profile Management Test** The user profile / user preference should be updated in the system.	FTP_TRP.1, FAU_GEN.1, FAU_GEN.2, FIA_ATD.1, FIA_SOS.1	Passed

Test ID	Description	Security Function	Results
Test-ATE-036	**Update Case Test** The incident/case details will be updated.	FTP_TRP.1, FAU_GEN.1, FAU_GEN.2, FDP_ACC.1, FDP_ACF.1	Passed
Test-ATE-037	**Update Task Test** The task details/status will be updated.	FTP_TRP.1, FAU_GEN.1, FAU_GEN.2, FDP_ACC.1, FDP_ACF.1	Passed
Test-ATE-038	**Virtual Patrol Test** CCTV that has been acknowledged will have the status updated as "Acknowledge"	FTP_TRP.1, FDP_ACC.1, FDP_ACF.1	Passed
Test-ATE-039	**Invalid User Access Test** The user is brought back to the mode selection page as user doesn't have access to the System Admin menu.	FTP_TRP.1, FAU_GEN.1, FAU_GEN.2, FDP_ACC.1, FDP_ACF.1	Passed

48 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Vulnerability Analysis

49 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

50 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a

Basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation

2.1.4.4 Vulnerability testing

51 The penetration tests focused on:

a) Insecure Channel

b) Authentication Bypass

c) Sensitive Content Discovery

d) Network Sniffing

e) Password Requirements

f) Password Brute Force

g) Black box scanning

h) XSS

i) SQLi

52 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in the Security Target (Ref [6]).

2.1.4.5 Testing Results

53 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all the test conducted were PASSED as expected.

3 Result of the Evaluation

54 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of MOzART Command Center Web Portal v1.1 which is performed by TÜV Austria CyberSecurity Lab Sdn. Bhd (TACSL).

55 TÜV Austria CyberSecurity Lab Sdn. Bhd (TACSL) found that MOzART Command Center Web Portal v1.1 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.

56 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

57 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.

58 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.

59 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

60 The Malaysian Certification Body (MyCB) is strongly recommended that:

a) the developer to implement a session timeout mechanism into the platform.

b) The developer to apply international standard hardening checklists on the platform's system environment to ensure secure configuration.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v1, CyberSecurity Malaysia, December 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2a, August 2020.

[6] MOzART Command Center Web Portal Security Target, Version 1.26, 11 May 2021.

[7] Evaluation Technical Report Certis CISCO MOzART Command Center Web Portal v1.3 ,2 July 2021.

A.2 Terminology

A.2.1 Acronyms

Table 5: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body

Acronym	Expanded Term
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 6: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65

Term	Definition and Source
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---