MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

C115 Certification Report

Argus Command Center Web Portal Stable Version 2.1

File name: ISCB-3-RPT-C115-CR-v1
Version: v1
Date of document: 16 JUNE 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

C115 Certification Report

Argus Command Center Web Portal Stable Version 2.1

16 JUNE 2021

ISCB Department

CyberSecurity Malaysia

Level 6, 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:	C115 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C115-CR-v1
ISSUE:	v1
DATE:	16 JUNE 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 23 June 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	7 June 2021	All	Initial draft
v1	16 June 2021	All	Final version

Executive Summary

The Target of Evaluation (TOE) is a web-based command center application of the Argus System called the Argus Command Center Web Portal (Argus CC) which provides the user for two primary purposes as an officer (security personnel) support system; security operations management and account management through the Internet.

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. and the evaluation were completed on 21 May 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 Argus Command Center Web Portal Stable Version 2.1 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 command center application of the Argus System called the Argus Command Center Web Portal (Argus CC) which provides the use for two primary purposes as an officer (security personnel) support system; security operations management and account management through the Internet. The user roles defined in the Argus CC consist of System Administrator, Account Owner, Managers, Operators, Supervisors and Officers. Supervisors and Officers are managed by TOE users but are themselves not TOE users and are thus omitted from the scope of this evaluation. Fundamentally, the TOE can be accessed by consumers via selected web browsers (front-end Command Center).

2 The TOE includes the following security functions:

- Identification & Authentication
- Security Management
- Trusted Path/Channels
- User Data Protection

1.2 TOE Identification

3 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C115
TOE Name	Argus Command Center Web Portal
TOE Version	Stable version 2.1
TOE Release Date	4th October 2019
Security Target Title	2019 Certis Cisco – Argus CC EAL2 – Security Target [ASE]
Security Target Version	V1.14
Security Target Date	18 February 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
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.

1.3 Security Policy

4 There is no organisational security policies defined regarding the use of TOE.

Table 2: Organizational Security Policies

P.PASSWORD	Authorized TOE users are required to use a combination of credentials (username and password) where the attribute of the password consists of (at least one) uppercase, lowercase, alphanumeric, special characters and a minimum length of 8 characters. All authorized TOE users are required to change the given temporary password during the following scenarios: a. First-time login b. When their existing password has been changed by TOE users (Managers, Account Owners) using the Change Password feature, which sends the temporary password to the users through their registered email address.
P.ACCESS_ROLE	Only authorized individuals that have been assigned with respective roles will be approved of access to the TOE and

	permitted to perform the corresponding functions of the TOE. Role-based assignment controls the functional usage of each user.
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

5 The TOE includes both physical and logical boundaries which are described in Section 2.5 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

6 The TOE consists of the following security functions identified in the Security Target (Ref [6]).

Table 3: TOE Logical Boundaries

Identification and Authentication	Argus CC will identify and authenticate the user before any actions can be performed. Mechanisms such as strong password requirement and account lockout are implemented to increase the difficulties of unauthorized access.
Security Management	Argus CC allows authenticated user to manage their own password. TOE user with higher privilege (e.g., Account Owner) will be able to manage the user account such as reset user's password.
Trusted Path/Channels	Argus CC has implemented a secure communication protocol where data communicated between TOE and user's web browser travels through an encrypted channel.

User Data Protection	Argus CC has implemented role-based access control (RBAS), where data be only view by the authorized party. Argus CC also implemented with appropriate data segregation where user can only access to data based on their assigned user role.

1.4.2 Physical Boundaries

7 Product components included in the TOE are listed below. Figure 1 illustrates a representative diagram of the TOE in its evaluated configuration.

- UI Layer
- Business Logic
- Web Browser

8 At a high level, the TOE process flow includes the following:

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

9 Argus System product components excluded from the TOE in the evaluated configuration are:

- Servers
- Databases
- Business components
- Third-party hosting platform (AWS)

10 The following diagram is a representation of the evaluated configurations of the TOE and its components.

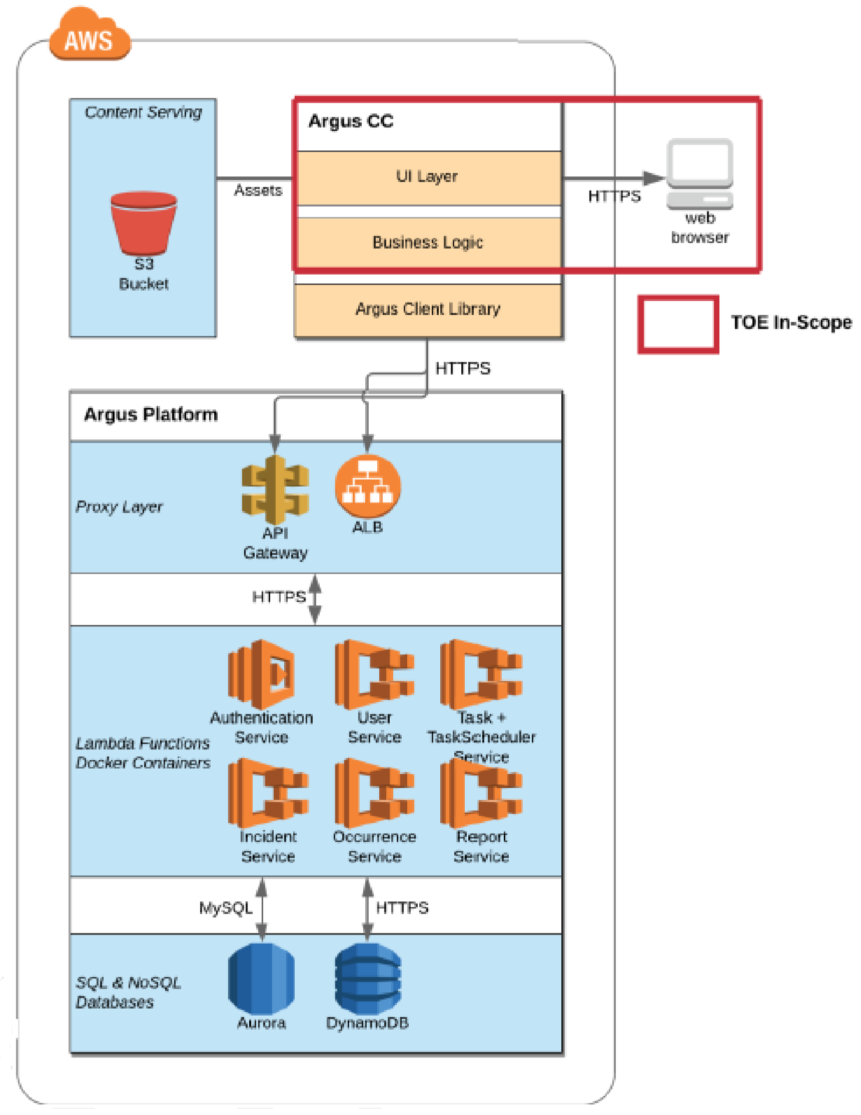

Figure 1: TOE Architecture

1.5 Clarification of Scope

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

12 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]).

13 Potential consumers of the TOE are advised that some functions and services of the overall product have not 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

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

1.6.1 Operational Environment Assumptions

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

Table 4: Assumptions for the TOE environment

Assumption	Statements
A.TRUSTED_ADMIN	The assumption is made that one or more competent, trusted personnel who are not careless, wilfully negligent, or hostile, are assigned and authorized as the TOE System Administrators, and do so using and abiding by guidance documentation. Authorized TOE System Administrators have no malicious intent; and are appropriately trained to undertake the configuration and management of the TOE.
A.TRUSTED_DEV	The assumption is made that the TOE development team has no malicious intent and will not wilfully modify the TOE with malicious exploits or misconfigure the TOE so as to compromise its security mechanisms.
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 Argus System to preserve accurate audit logs. The audit logs are considered out of TOE scoping.

Assumption	Statements
A.CLOUD	The assumption is made that the cloud service provider that provides the IT infrastructure of the TOE is fully capable of providing a physically secure environment (data center) that limits access to authorized personnel. The cloud service provider will not willfully tamper with the TOE or gain access to the contents of the TOE.
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 the platform and network environment on which the TOE operates shall be secure against DDoS attacks.
A.CONNECTIVITY	The assumption is made that the TOE uses a secure and trusted Internet connection.
A.THIRDPARTY	The assumption is made that all integrated third-party data communicated between the TOE maintains integrity.

1.7 Evaluated Configuration

16 The TOE's evaluated configuration provides the access and usage of the Argus CC modules and functions directly. The TOE's primary function is to provide consumers with an advanced but user-friendly interface that eases the monitoring and managing of their accounts. These include functions such as monitoring of security operations and managing users and tasks within their accounts. The target audience of the ST encompasses consumers who are interested in maintaining and controlling a dynamic platform that allows operations planners to break down security workflows into logical series of tasks and to define the conditions necessary to fulfil those tasks.

17 The Argus CC allows consumers to have a complete command-and-control (C2) officer support system that actively monitors the activities and wellbeing of security officers. The TOE can only be used authenticated users via web browsers. Customers will need

to obtain the account username and password from Argus's System Administrator in order to use the TOE.

18 The TOE is an internal operations system and it is not sold as a commercial product. Internally, Argus CC is provisioned on a software as a service-like model (SaaS), which means new accounts are given Account Owner login credentials, which they will use to manage their accounts.

19 The TOE software is installed together with the rest of the Argus System onto the AWS cloud environment. Specifically, for the TOE, its components are hosted in Amazon S3 (object storage service) and distributed by Amazon CloudFront. It is assumed that the installation of the TOE is secure and that the TOE software is not susceptible to unauthorized modification by attackers, other tenants or even the cloud service provider.

20 With reference to Sec. 1.3.2 of 2019 Certis Cisco – Argus CC EAL2 – Delivery [ALC_DEL.1] supporting document, users of the TOE access Argus CC over the Internet using any of the supported modern web browsers listed in Sec. 2.4. The TOE must be accessed over an encrypted HTTPS channel using TLS 1.2, as mandated by Amazon S3 and Amazon CloudFront. The TOE does not support unencrypted access over HTTP. There is no additional hardware requirement to access the TOE, for example, using hardware security tokens. Securely accessing the TOE ensures that its source code is not tampered with, which could lead to the TOE exhibiting unexpected behaviors.

21 As a web-based application, the TOE is rendered (HTML) and executed (JavaScript) by web browsers. It is assumed that the web browsers and operating systems used by TOE users are secured and do not have malicious agents that can access the TOE's content or snoop around the data transmission.

22 The installation of the TOE is performed by the Argus Preparative Team. After initial configuration, the TOE is handed over to the appointed System Administrator, with guidance documents described in the following table. Other than the System Administrator, other TOE users of different roles are also provided guidance on how to access and use the functions available to them.

1.8 Delivery Procedures

23 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.

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

1.8.1 TOE Delivery

25 The Argus Command Center Web Portal (the TOE) is the operations and administration frontend of the Argus platform (non-TOE system), which is a command-and-control system for physical security operations.

26 The TOE is readily available to the end-user and runs within the context of web browsers, as it is implemented as a web application (single-page HTML application). The interfaces listed above are Graphical User Interfaces implemented as HTML pages. TOE users interact with these interfaces, or web forms, through modern web browsers, with the assumption that the operating environment is secure and safe from malware that can modify the TOE's behaviour or intercept communication.

27 Access to the TOE which involves the landing page URL and credentials, are electronically distributed to the user with System Administrator role through email after a system administrator has carried out creation of the user. This includes links to download the user guidance documentation. Users that have the Account Owner, Manager or Operator role also receive access to the TOE through electronic mail after the users have been created.

2 Evaluation

28 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 ISCB Product Certification Schemes Policy (Product_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

30 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the TOE provided for evaluation is labelled with its reference and the TOE references used are consistent.

31 The evaluators examined that the method of identifying configuration items and determined that it describes how configuration items are uniquely identified

32 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the 2019 Certis Cisco - Argus CC EAL2 - Configuration Management Scope [ALC_CMS.2] version 1.7.

2.1.2 Development

Architecture

33 The evaluators examined the security architecture description and 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.

34 The security architecture description describes the security domains maintained by the TSF.

35 The initialisation process described in the security architecture description preserves security.

36 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

Functional Specification

37 The evaluators examined the functional specification and determined that:

- The TSF is fully represented;
- It states the purpose of each TSF Interface (TSFI); and
- The method of use for each TSFI is given.

38 The evaluators also examined the presentation of the TSFI and determined that:

- It completely identifies all parameters associated with every TSFI;
- It completely and accurately describes all parameters associated with every TSFI; and
- It completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

39 The evaluators also confirmed that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

TOE Design Specification

40 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems.

41 The evaluators also determined that all subsystems of the TSF are identified.

42 The evaluators determined that interactions between the subsystems of the TSF were described.

43 The evaluators examined the TOE and determined that each SFR supporting or SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is not SFR-enforcing.

44 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

45 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

46 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

47 The evaluators determined that all SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

48 The evaluators examined the operational user guidance determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

49 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

50 The evaluators examined the operational user guidance in conjunction with other evaluation evidences and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

51 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

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

2.1.4 IT Product Testing

53 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. The detailed testing activities, including

configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

54 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

55 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.

56 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 5: Independent Functional Test

TEST ID & RELATED SFRs	DESCRIPTIONS	RESULTS
Test-ATE-001 FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_SOS.2 FIA_UAU.1 FIA_UID.1 FTP_ITC.1	Conduct test case ID ***[Test-UL-1]*** specified in the developer's test documents to validate developer's test result. The TOE user should be redirected to the Administrator Console.	Passed. Result as expected.

TEST ID & RELATED SFRs	DESCRIPTIONS	RESULTS
FTP_TRP.1		
Test-ATE-002 FIA_ATD.1 FIA_UID.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	Conduct test case ID ***[Test-SA-1]*** specified in the developer's test documents to validate developer's test result. The Administrator Console should refresh, and the list of existing accounts will be displayed, along with the newly created account.	Passed. Result as expected.
Test-ATE-003 FIA_ATD.1 FIA_UID.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	Conduct test case ID ***[Test-SA-4]*** specified in the developer's test documents to validate developer's test result. The Administrator Console should refresh, where the list of existing account owners will be displayed, along with the user whose details were just updated.	Passed. Result as expected.
Test-ATE-004 FIA_SOS.1	Conduct test case ID ***[Test-SA-5]*** specified in the developer's test documents to validate developer's test result.	Passed. Result as expected.

TEST ID & RELATED SFRs	DESCRIPTIONS	RESULTS
FIA_SOS.2 FIA_UID.1 FMT_MSA.1 FMT_SMF.1 FMT_SMR.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	The Administrator Console will be refreshed, and the list of existing account owners will be displayed.	
Test-ATE-005 FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_SOS.2 FIA_UAU.1 FIA_UID.1 FTP_ITC.1 FTP_TRP.1	Conduct test case ID ***[Test-PR-1]*** specified in the developer's test documents to validate developer's test result. The popup with title "Request sent successfully!" should be displayed and when "Close" is clicked, it should redirect the TOE user to the Login page.	Passed. Result as expected.
Test-ATE-006 FIA_ATD.1 FIA_UID.1 FMT_MSA.1 FMT_SMF.1 FMT_SMR.1 FTP_ITC.1	Conduct test case ID ***[Test-AO-1]*** specified in the developer's test documents to validate developer's test result. The TOE user should be directed back to the Account Owner Portal's organization menu, where the list of existing organizations will be displayed, along with the newly created organization.	Passed. Result as expected.

TEST ID & RELATED SFRs	**DESCRIPTIONS**	**RESULTS**
FTP_TRP.1 FDP_ACC.1 FDP_ACF.1		
Test-ATE-007 FIA_ATD.1 FIA_UID.1 FMT_MSA.1 FMT_SMF.1 FMT_SMR.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	Conduct test case ID ***[Test-AO-4]*** specified in the developer's test documents to validate developer's test result. The TOE user should be directed back to the Account Owner Portal's account user's menu, where the list of existing users will be displayed, along with recently updated user.	Passed. Result as expected.
Test-ATE-008 FTP_ITC.1 FTP_TRP.1	Conduct test case ID ***[Test-AO-6]*** specified in the developer's test documents to validate developer's test result. The TOE user should be directed back to the Account Owner Portal's account users menu, where the list of existing users will be displayed, along with recently created user.	Passed. Result as expected.
Test-ATE-009 FIA_UID.1 FMT_MSA.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1	Conduct test case ID ***[Test-AO-8]*** specified in the developer's test documents to validate developer's test result. The TOE user should be redirected back to the Account Owner Portal's account user menu, where the list of existing account owners will be displayed, along with the suspended user. The suspended user should have a "Inactive" status displayed.	Passed. Result as expected.

TEST ID & RELATED SFRs	DESCRIPTIONS	RESULTS
FDP_ACF.1		
Test-ATE-010 FIA_UID.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	Conduct test case ID ***[Test-MG-1]*** specified in the developer's test documents to validate developer's test result. The TOE user should be redirected to the Operator Console's officer monitoring menu, where the list of users that exist in the account the Manager is currently signed in to as well as a map displaying the last known locations of each online officer.	Passed. Result as expected.
Test-ATE-011 FIA_UID.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	Conduct test case ID ***[Test-MG-6]*** specified in the developer's test documents to validate developer's test result. The TOE user should be redirected to the Manager Portal's task templates page, where the list of task templates in the organization will be displayed, along with the recently created task template.	Passed. Result as expected.
Test-ATE-012 FIA_ATD.1 FIA_SOS.1 FIA_SOS.2 FIA_UID.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1 FTP_ITC.1 FTP_TRP.1	Conduct test case ID ***[Test-MG-12]*** specified in the developer's test documents to validate developer's test result. The TOE user should be directed back to the Manager Portal's user's menu, where the list of existing users will be displayed, along with recently created Officer.	Passed. Result as expected.

TEST ID & RELATED SFRs	DESCRIPTIONS	RESULTS
FDP_ACC.1 FDP_ACF.1		
Test-ATE-013 FIA_UID.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	Conduct test case ID ***[Test-MG-16]*** specified in the developer's test documents to validate developer's test result. The TOE user should be redirected to the Operator Console's incident monitoring page, where the list of incidents in the organization will be displayed, along with the recently created incident.	Passed. Result as expected.
Test-ATE-014 FIA_UID.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	Conduct test case ID ***[Test-OP-1]*** specified in the developer's test documents to validate developer's test result. The TOE user should be redirected to the Operator Console's officer monitoring menu, where the list of users that exist in the account the Manager is currently signed in to as well as a map displaying the last known locations of each online officer.	Passed. Result as expected.
Test-ATE-015 FIA_UID.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	Conduct test case ID ***[Test-OP-3]*** specified in the developer's test documents to validate developer's test result. The TOE user should be redirected to the Operator Console's incident monitoring menu, where the list of existing incidents will be displayed. It is possible to have zero incidents created.	Passed. Result as expected.

TEST ID & RELATED SFRs	DESCRIPTIONS	RESULTS
Test-ATE-016 FIA_UID.1 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	Conduct test case ID ***[Test-OP-6]*** specified in the developer's test documents to validate developer's test result. The TOE user should be redirected to the Operator Console's task monitoring page, where the list of tasks in the organization will be displayed, along with the recently created task.	Passed. Result as expected.
Test-ATE-017 FTP_ITC.1 FTP_TRP.1 FDP_ACC.1 FDP_ACF.1	Conduct test case ID ***[Test-OP-8]*** specified in the developer's test documents to validate developer's test result. The TOE user should be redirected to the Operator Console's incident monitoring page, where the list of incidents in the organization will be displayed, along with the recently created incident.	Passed. Result as expected.

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

2.1.4.3 Penetration Testing

58 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.

59 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) Any public knowledge of the vulnerability or known exploit;

b) The complexity of the vulnerability and its identification;

c) The exploitability of the identified vulnerability;

d) The time required to perform the exploit of vulnerability;

e) Level of knowledge towards the TOE; and

f) Additional resource(s), if any, required for an exploitation

60 The penetration focused on:

a) Insecure Channel;

b) Authentication Bypass;

c) Content Discovery;

d) Network Sniffing;

e) Password Requirement;

f) Password Brute Force; and

g) Black Box Scan.

61 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in Section 1 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

62 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 tests conducted were PASSED as expected.

3 Result of the Evaluation

63 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 Argus Command Center Web Portal Stable Version 2.1 performed by TÜV AUSTRIA CYBERSECURITY LAB SDN. BHD.

64 TÜV AUSTRIA CYBERSECURITY LAB SDN. BHD. found that Argus Command Center Web Portal Stable Version 2.1 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.

65 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

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

67 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.

3.2 Recommendation

68 The Malaysian Certification Body (MyCB) is strongly recommending 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] 2019 Certis Cisco – Argus CC EAL2 - Security Target, Version 1.14, 18 February 2021.

[7] Certis CISCO Argus Command Center Web Portal Draft, Evaluation Technical Report, Version 1.2, 14 June 2021.

[8] 2019 Certis Cisco – Argus CC EAL2 TOE Design Documentation, Version 1.9, 7 May 2021

A.2 Terminology

A.2.1 Acronyms

Table 6: 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
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile

Acronym	Expanded Term
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 7: 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
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.

Term	Definition and Source
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 ---