CERTIS

Argus Command Center Web Portal
Security Target [ASE]
(v1.14)

CERTIS CISCO SECURITY PTE LTD

Evaluation Assurance Level 2

CONFIDENTIAL

[BLANK PAGE]

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

Document Details

Version	Date	Description	Author
1.0	22th of October 2019	Security Target (ST) generated with required document template.	Lai Yeong Hin
1.0	22th of November 2019	Added Chapter 1 to Chapter 4.	Samuel
1.1	4th of December 2019	Review Chapter 1 and 4.	Lai Yeong Hin and Consultant
1.2	7th of December 2019	Add Chapter 5 Threat, Organizarional Security Policiesand Assumptions.	Samuel
1.3	19th of December 2019	Review and changes made in Chapter 5 Threats, Organizarional Security Policies, and Assumptions to the ST.	Lai Yeong Hin and Consultant
1.4	6th Jan 2020	Add Chapter 6. And Chapter 7 Security Functional Requirement.	Samuel
1.5	2nd Feb 2020	Review and changes made in Chapter 6 and 7. Added Chapter 8 Security Assurance Requirements to the ST.	Lai Yeong Hin and Consultant
1.6	5th March 2020	Request additional information into Chapter 7. Review and confirm Chapter 8 Security Assurance Requirements. Add Chapter 9 TOE Summary Specification.	Samuel
1.7	8th March 2020	Review and changes made on Chapter 7. Review and changes made on Chapter 9.	Lai Yeong Hin and Consultant
1.8	9th March 2020	Changes made on Chapter 7 and Chapter 9.	Samuel
1.9	14th March 2020	Review Chapter 7 and Chapter 9.	Lai Yeong Hin and Consultant
1.10	18th March 2020	Changes made on Chapter 9.	Samuel
1.11	19th March 2020	Finalised the document.	Lai Yeong Hin and Consultant, Samuel
1.12	25 Aug 2020	Amended according to Draft Evaluation Observation Report 1.0 dated 8 Jul 2020.	Samuel Low
1.13	6 Nov 2020	Amended according to feedback from Evaluation Observation Report 1.0 dated 27 Oct 2020.	Samuel Low
1.14	18 Feb 2021	Update the naming of AGD supporting document	Claire Chou
1.14	4th May 2021	Updated number of characters relating to secrets and passwords	Dominic Soh

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	2019 Certis Cisco – Argus CC EAL2 – Security Target [ASE]-v1.14
ST Identifier	Argus-Command-Center-Web-Portal_ST_EAL2_v1.14
ST Version/Date	v1.14, 18th of Febuary 2021
TOE Title	Argus Command Center Web Portal
TOE Version	Stable Version 2.1
TOE Date of Release	4th of 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 • 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 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 frwom the scope of this evaluation. Fundamentally, the TOE can be accessed by consumers via selected web browsers (front-end Command Center).

References to **Argus System** or **Argus Platform** within the ST and EAL2 supporting documents refer to the entire Argus application which comprises the TOE – **Argus Command Center Web Portal** (abbreviated as **Argus CC**) and non-TOE supporting systems. To be clear, the terms **Argus System** and **Argus CC** are not equivalent and appropriate distinction ought to be considered whenever these terms are used.

2.1 TOE USAGE AND MAJOR SECURITY FEATURES

The target audience of the ST encompasses consumers who are interested in maintaining and controlling a dynamic tasking 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. Argus CC allows consumers to have a complete command-and-control (C2) officer support system that actively monitors the activities and well-being of security officers.

The TOE is capable of performing the following functions upon successful authentication.

Function	Description
OPERATOR CONSOLE	
Task Monitoring (Task assignment and progress monitoring)	
Task Assignment and Monitoring	• Allows Operators to create, assign task to security officers. • Progress monitoring on security officer. • Create a new task for a respective security personnel.
Report Generation	• Argus CC allows Managers to peruse a slew of operational reports. However, Argus CC does not allow for downloading or exporting of reports. • The reporting function generates as a list of rows summarizing data from the Task Reports to be viewed electronically.
Incident Report (React to incident at single touch)	
Incident Response	• Used to provide incident response work flows such as assign, create, report and query incidents. • Allow Operators to handled reported incidents by assigning tasks to security officers, create their own feedback into incidents and forward the message to ther Operators. • Create and report a new incident.
Report Generation	• Argus CC allows Managers to peruse a slew of operational reports. However, Argus CC does not allow for downloading or exporting of reports. • The reporting function generates as a list of rows summarizing data from the Incident Reports to be viewed electronically.
Officer Monitoring (Near real-time location updates)	
User Monitoring	• Real-time monitoring for security officer. • Locate security officers. • Monitor progress of task completion by security officers.

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

	• Query security personnel's monitoring details.
Messaging (Send messages to officers)	
Messages	• Operators are capable of send messages to 1 or many (groups) of Officers. • Used as a form of acknowledgement from Officers.
Report Generation	• Argus CC allows Managers to peruse a slew of operational reports. However, Argus CC does not allow for downloading or exporting of reports. • The reporting function generates as a list of rows summarizing data from the Messaging to be viewed electronically.
MANAGER PORTAL (Plan tasks, duty packages and incident categories)	
User Management	• Within an organization, Managers can manage users, which represent the security officers. Managers can also create and manage Operators. • Operators can only access the operations features of Argus CC and do not have the necessary permissions to perform user management. • User Groups offer a way to logically separate different groups of users in a hierarchical manner, for example, based on teams or duty shifts. • Managers have the ability to create users, either using the user interface or importing users en masse using the Import CSV function. Minimally, the fields required are the Employee ID (username), email address and phone number. This process onboards the users into the system but does not specify any credentials. Users will have to create their credentials from the Argus mobile applications.
Task Planner	• Argus CC provides a comprehensive tool to manage Task Templates, which can be thought of as the blueprints for tasks. • Operations planners define the routines that have to be performed in task templates and the groups of users that are qualified to perform those routines. • The counterparts to task templates are Duty Plans, which dictate when tasks are to be created, and to automatically assign them. Task templates, combined with duty plans, enable Managers to express complex operational workflows.
Data Management	• Operational data in the Argus System contains categorical fields such as the types of incidents, the types of tasks, locations and duty posts. This categorical information has to be defined before being used in tasks and incidents.
Occurrence Book (View electronic occurrence entries)	
LogBooks	• View electronic occurrence entries through the security personnels' logbook of routine activities.
Report Generation	• Argus CC allows Managers to peruse a slew of operational reports. However, Argus CC does not allow for downloading or exporting of reports. • The reporting function generates as a list of rows summarizing data from the Logbooks to be viewed electronically.
ACCOUNT OWNER PORTAL (Manage and configure an Account)	
Organization Structure Management	• Account Owners to have the ability to create organizations and to effectively manage the hierarchical organization structure in their accounts. • Organizations are the means to segregate operational data and oftentimes, they represent actual real-world locations, such as shopping malls and airports. • Only Account Owners can create Managers and assign them to organizations. Cascading downwards, the management of an organization is the responsibility of its assigned Managers.
User Management	• Create Managers and assign them to Organizations

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

ADMINISTRATOR CONSOLE (Manage Accounts at a system level)	
Account Management	• Create and manage Accounts on the Argus system, where each Account is segregated from other Accounts • Create Account Owners and assign them to Accounts

In summary, the TOE, Argus CC, is a web application that provides a rich and highly interactive user interface that aims to ease the job that users have to carry out in maintaining an officer (security personnel) support system. The TOE acts as the main user interface for consumers (in their respective roles as a System Administrator, Account Owner, Managers, Operators, Supervisors and Officers) to carry out operational features (task assignment and monitoring, incident responses, user monitoring) and management features (account management, organization management, user management, task planner, data management, report generation) within Argus CC itself. The rest of the components within the Argus system such as the server, database, business components and third-party hosting platform, Amazon Web Service (AWS), are deemed as out of the TOE scope.

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

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

2.2 SUPPORTING NON-TOE HARDWARE

The Argus system contains a series of supporting non-TOE hardware which provisions the 6 distinct components of the entire system itself (emphasized in the sub-section below). The supporting non-TOE hardware primarily consists of a third-party hosting environment called the Amazon Web Service (AWS) which accommodates and contains all necessary components of the Argus system.

In this scenario, the Argus system is considered as a serverless state as all management of Argus system infrastructure is conducted solely by Amazon Web Services, Inc.

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

- Amazon Web Service (AWS) host,
- database host(s);
- mobile device(s).

Hardware	Specification
Amazon Web Service (AWS) Host	Authentication Service: AWS Lambda Every other service: AWS Elastic Container Service running on c4.xlarge EC2 instances
Database Host(s)	Amazon RDS Engine: Aurora MySQL Multi-AZ Size: db.r4large (2 x vCPU, 15.25GB RAM)
	AWS ElastiCache Mode: Redis Size: cache.m4.large (2 x vCPU, 6GB RAM)
	Amazon DynamoDB
Mobile Device(s)	OS: Android 7 and above RAM: Minimum 2GB CPU: Dual-core
Web Browser(s)	OS: Windows 7 or later, MacOS 10.10 or later RAM: Minimum 4GB

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

	At least Chrome 62 and Firefox 52

2.3 SUPPORTING NON-TOE SOFTWARE

The Argus System is comprised of 6 distinct components (depicted as numbered items within a purple circle in the image below). Out of these 6 distinct components, 5 of them are deemed as supporting non-TOE software. Most of the components that makes up for the Argus system (Component 1, 2, 3 and 4) are located inside the Amazon Web Services AWS S3 (AWS), a third-party hosting environment which is deemed as out of scope. Component 5 is also out of scope.

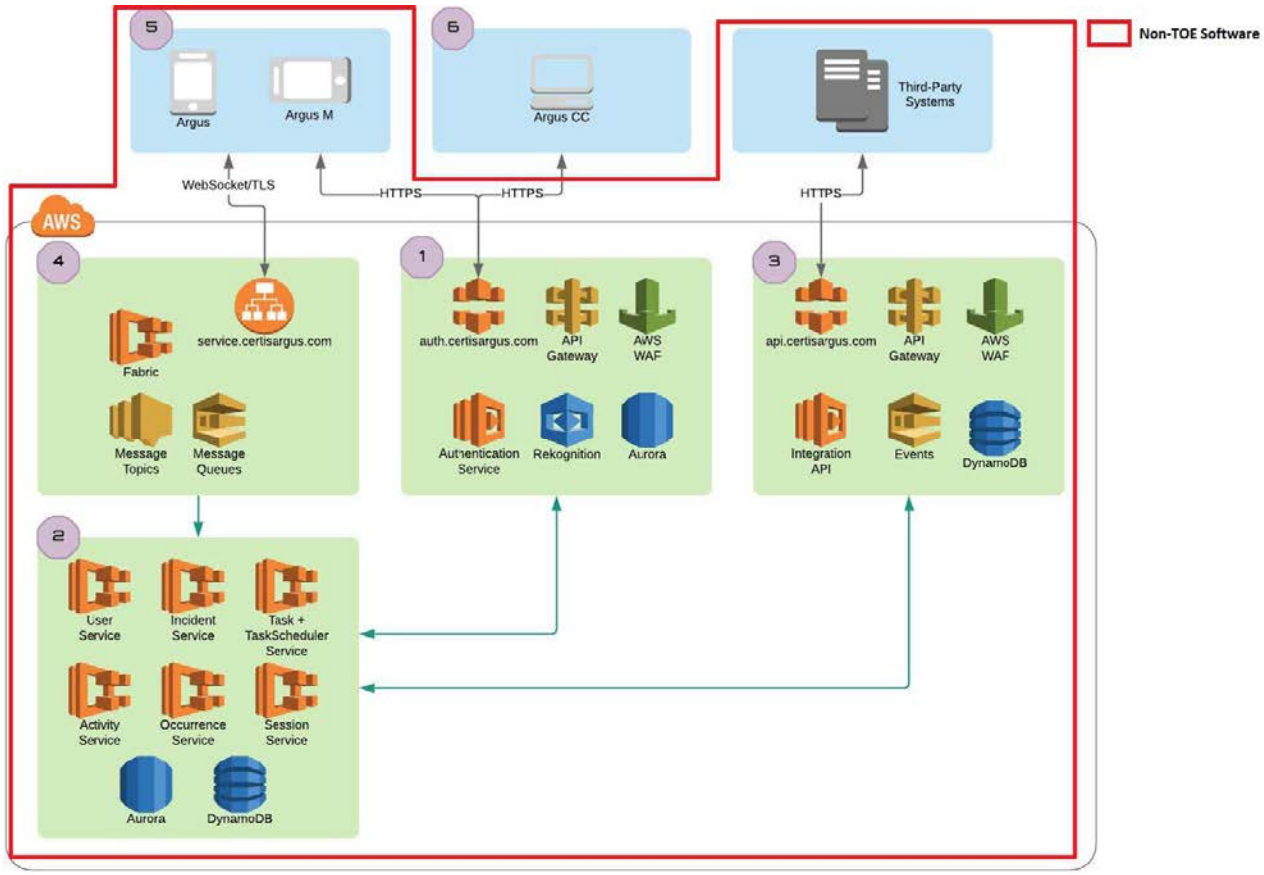

Figure 1 shows the supporting non-TOE software shown within the red box above.

Software	Version	Description
Authentication Service	1.0.0	Component 1. This component provides authentication services for authorized users of the Argus System, including Argus CC (the TOE). It supports two forms of authentication method – passwords and biometrics (facial recognition, non-TOE). Authenticated users are tagged with their assigned roles. User sessions are encoded using JSON Web Tokens and digitally signed.
Task Management Platform	2.0.0	Component 2. The Task Management Platform is a secure, multi-tenant server application that executes the myriad of business logic encompassing the operational workflows provided by the Argus System. It is composed of seven separate services that work

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

		together to provide the functionalities available in the Argus Platform. • Authentication service • User service • Task service • Incident service • Occurrence service • Session service • Dashboard service
Integration API	1.4.1	Component 3. The Integration API exposes service commands and events to third-party systems that integrate with the Argus System. It is a rich REST-based API that offers those systems the ability to obtain information about the current state of various entities and also to execute actions on those entities. Entities are object models such as Users and Tasks. The Integration API is secured at the transport layer using HTTPS/TLS and authenticated using API keys and IP whitelisting. The Integration API is protected from denial-of-service (DoS) attacks using AWS API Gateway's request throttling feature and AWS Shield which is a managed DDoS protection service.
Messaging Middleware (Fabric)	1.0.0	Component 4. The Messaging Middleware, which the development team has termed as "Fabric", is an innovative combination of SNS and SQS to achieve real-time pub-sub messaging with FIFO and at-most-once processing semantics. Using this middleware, message routing can be configured at the infrastructure level instead of the application level. Messages can be "fanned out" by adding subscribers to outgoing SNS topics. For example, messages can be routed to SIEM applications, in addition to backend processing services. Additionally, message durability is intrinsic in the system due to the message queue, that is, there will not be data loss even when message consumers are not available.
Mobility Applications	Argus System Officer Mobile App 1.2 Argus System Supervisor Mobile App 1.2 Samsung Knox	Component 5. The Mobility Applications are Android applications that serve as the frontends of the Argus System. Security ground staff interact with these applications throughout the course of their working day. Stringent data security is enforced by the applications due to the sensitive nature of security operations, for example, the tasks being done at certain critical infrastructure sites. From the perspective of data security, no sensitive operations data is stored in the mobile applications. Once security officers go off-duty and signs out of the Argus system, no data related to their work is retained. The devices are managed using Samsung Knox, which is a premium Mobile Device Management solution from Samsung. Samsung Knox allows remote management of the devices and can perform remote wiping of devices.

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

Argus Command Center Web Portal	Argus Command Center Web Portal Version 2.1	Component 6. **This is the TOE itself**. This component is the web application of the Argus System used primarily in the command center. There are two main groups of users – Operators and Managers. Operators use Argus CC to monitor and supervise ongoing security operations. Such duties include: • Assign tasks to security officers • Monitor well-being and activity of security officers • Respond to incidents reported by security officers • Disseminate relevant information Managers perform administrative duties that primarily describe the custom operational data and processes for their assigned organizations. Only Managers can access the Administrative Portal within the Argus Command Center Web Portal. Within the Administrative Portal, Managers can perform the following actions. • Manage users and user groups • Maintain operations metadata • Define task templates • Schedule duty plans • Generate reports Account Owners perform administrative tasks related to their assigned Account. Their primary responsibilities are to manage users and organizations within the Account, through the following actions. • Manage users and managers • Manage organizations • Manage organization structure

2.4 CLIENT REQUIREMENTS

The respective components within are required for the TOE to work as intended:
- Angular framework (Version 6)
- CSS frameworks
- Bootstrap UI component library

The TOE supports the following types of web browsers:
- Google Chrome 62 or later
- Mozilla Firefox 52 or later

A web browser that supports the components and matches the use of appropriate web browser types listed above will be able to access the TOE. With that said, both the components and web cookies must be enabled to facilitate web portal sign-ins.

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

The TOE officially supports Chrome 62 and Firefox 52 or later. Other web browsers such as Internet Explorer, Edge, Safari are not officially supported. Usage of TOE through the unofficial web browsers may be possible but expected performance may not be working as intended.

The TOE adopts the Single-Page Application (SPA) model. The application code and resources are mostly retrieved in the initial page load, with additional resources dynamically loaded and added to the page as necessary. The TOE, Argus Command Center Web Portal interacts with Argus services using REST-based requests over a secure communications channel, Hyper Text Transfer Protocol Secure (HTTPS).

2.5 TOE DESCRIPTION

2.5.1 Physical Scope of the TOE

The TOE is a web-based application hosted on Amazon Web Services Simple Storage Service (Amazon S3) and distributed through Amazon CloudFront, which is a content distribution network (CDN). Users of the TOE access Argus CC using modern web browsers, running on computer systems in the secure premise of an operations command center. The rest of the components within the Argus System such as the servers, databases, business components and third-party hosting platform (AWS), 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

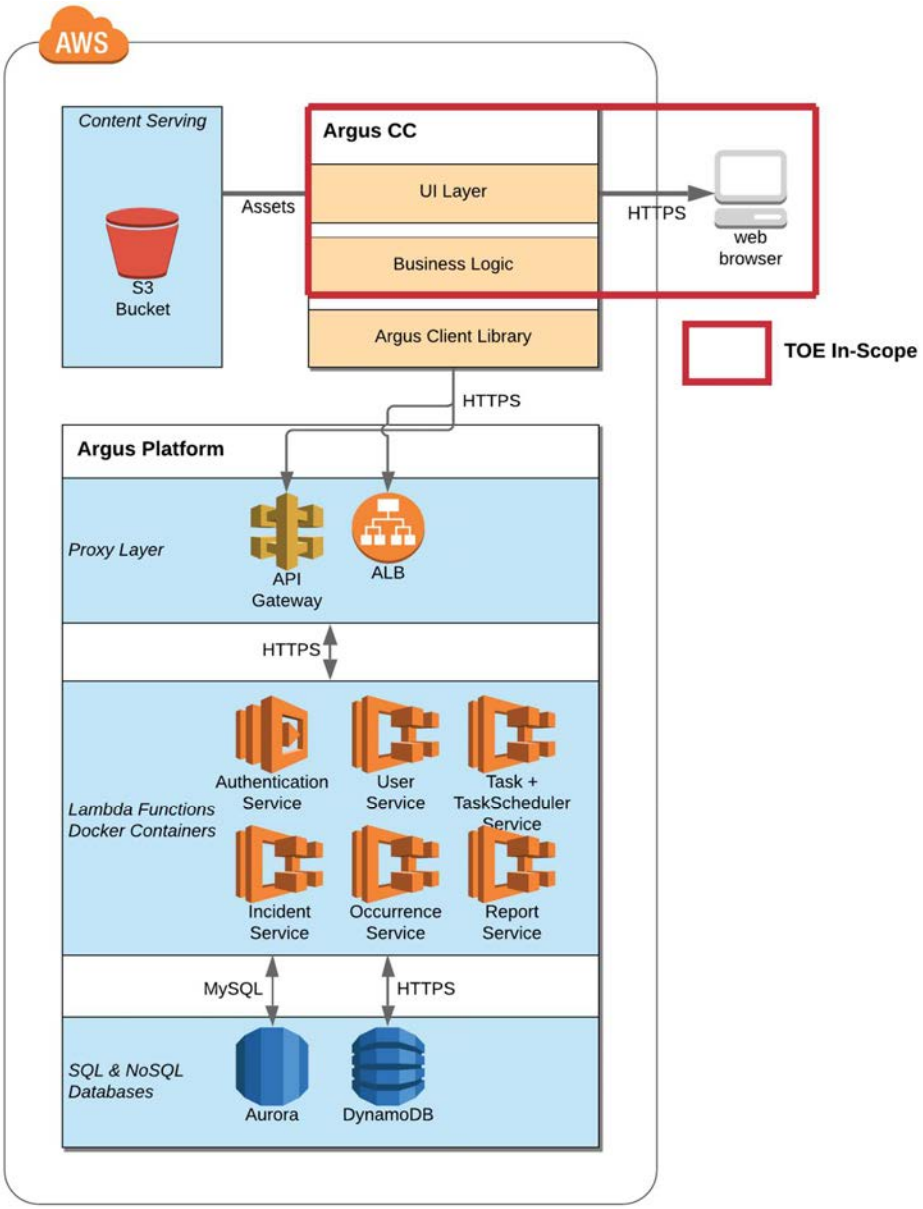

Figure 2 shows the detailed phyiscal architecture of the entire Argus System deployed in the AWS hosting environment, listing the AWS services being used. The Argus Platform and AWS S3 are deemed as out of scope.

Consumers are able to access the TOE upon successful authentication through the web browser and perform the TOE's intended operations. No additional installation or setup is required to access the functions of the TOE. The TOE is not sold as a whole product and is meant for internal corporate usage only.

The diagram below depicts the entire Argus 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

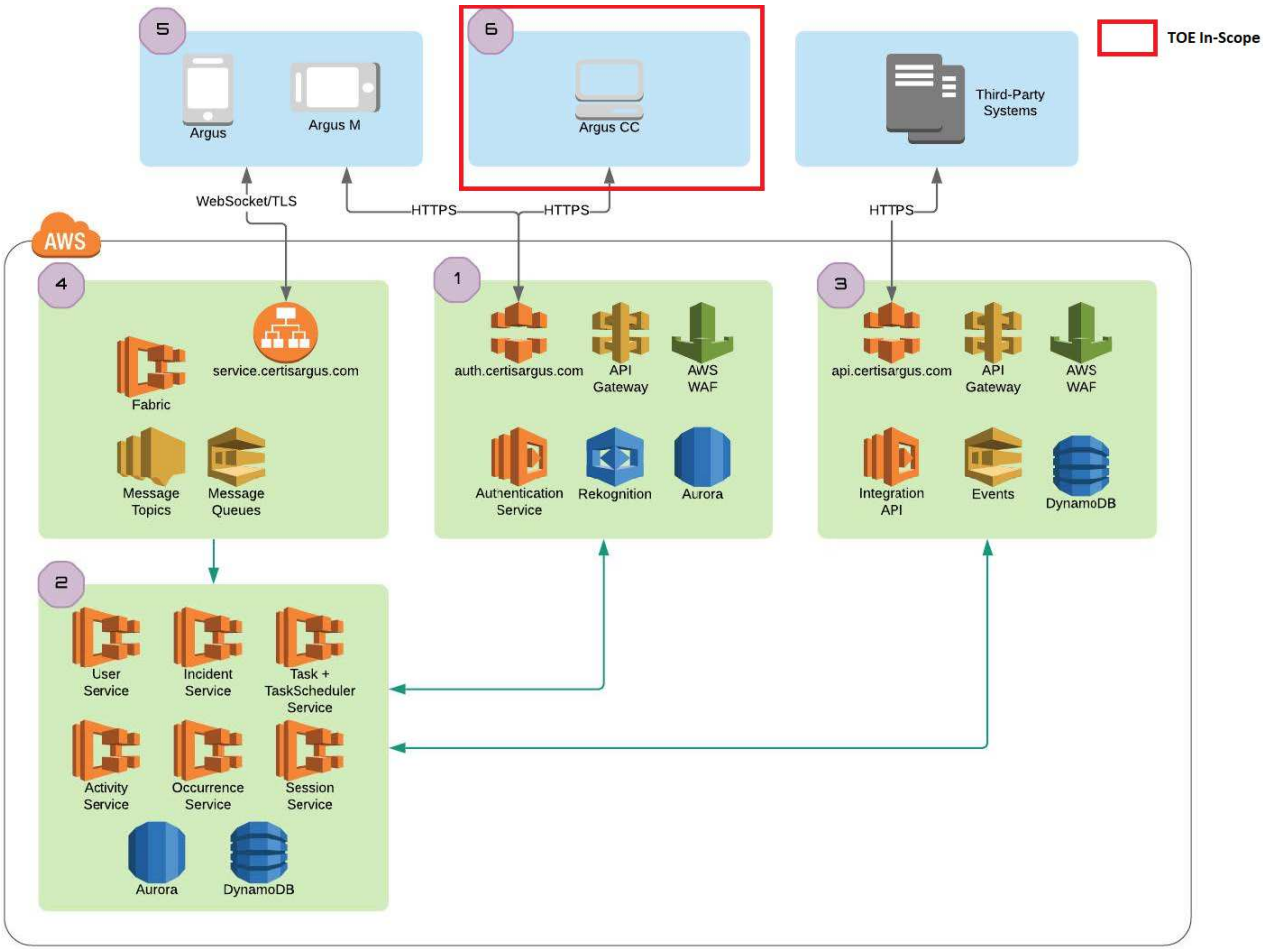

Figure 3 shows the Argus System architecture, with logical scope of the TOE, Argus Command Center Web Portal boxed in red above.

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

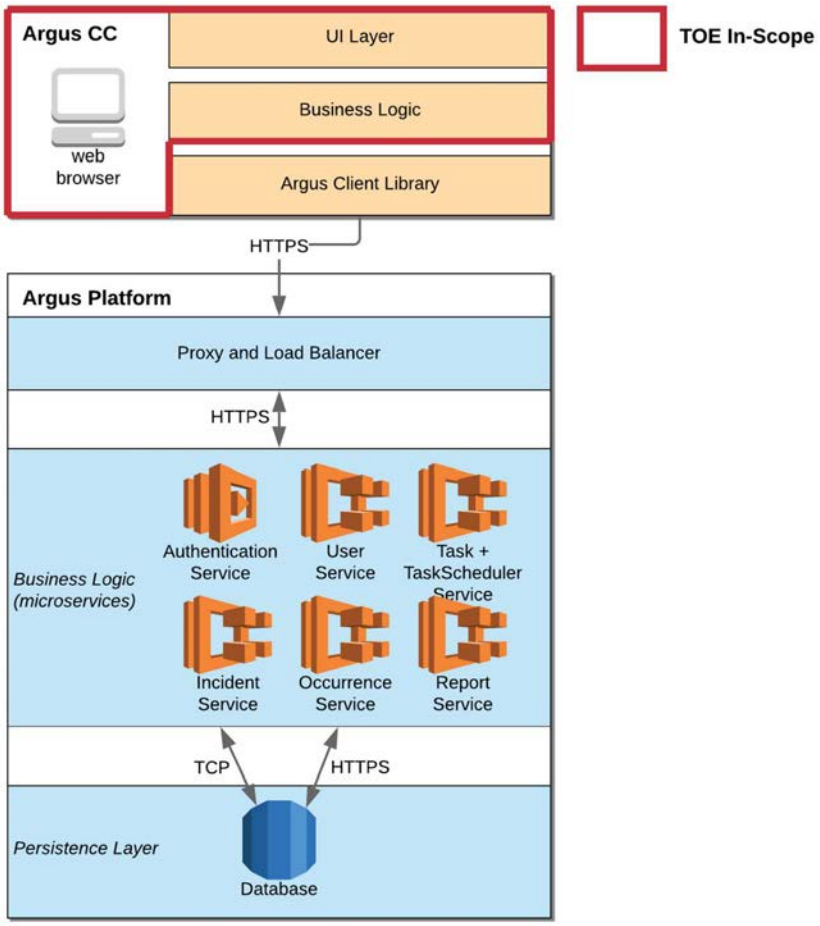

Figure 4 shows the detailed application architecture together with the logical scope of the TOE boxed in red. The Argus Platform is deemed as out of scope.

All hardware appliances/devices, software components, integration APIs and third-party hosting environment (AWS) used to support the TOE are not part of the scope of evaluation. The Argus Client Library (ACL) in the diagram above (Figure 4) is a software development toolkit (SDK) used to ease the development of client-side applications which is also considered not in-scope. Every other component that is not boxed in the above diagrams (refer to Figure 2 and Figure 3) are considered not in-scope.

The TOE in-scope 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 Argus 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. 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 used by 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.

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.

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

2.5.1.1 Software

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 susceptiable to unauthorized modification by attackers, other tenants or even the cloud service provider.

2.5.1.2 Secure Access

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.

2.5.1.3 Runtime Environment

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.

2.5.1.4 Delivery and Usage Guidance

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.

Document	Description
2019 Certis Cisco – Argus CC EAL2 – Delivery [ALC_DEL.1]	• Provided by the Argus Preparative Team to the System Administrator of the TOE to verify that the TOE is correctly installed and configured. • Provides information on procedure for issuance of accounts, TOE confidentiality and availability.
2019 Certis Cisco – Argus CC EAL2 - Operational User Guidance [AGD_OPE.1] & Preparative Procedure [AGD_PRE.1]	• Provides detailed instructions on how to use the functions in the TOE with respect to the assigned role of the TOE user, e.g. System Administrators accessing the functions of the Administrator Console, Operators accessing the functions of the Operator Console. • Provides details on installation and acceptance criteria of the TOE, which should be verified by the System Administrator.

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	Description
Identification and Authentication	Authentication and authorization are enforced • TOE identifies and authenticates users before the users are allowed to perform any actions within the TOE. • TOE provides unidentified users a method to recover their accounts. • Authenticated TOE users are allowed to change their own password. • TOE is capable of handling security concerns over the use of username/password credentials combination to authenticate through the Command Center. • TOE has a set of password rule and policies which strengthens the complexity of an authentication. • TOE handles authentication failures by temporarily locking down user accounts.

Security Attribute Management	Security attribute management, including user credentials and authorization
	• TOE supports the management of user's security attributes.
	• TOE stipulates a fixed set of roles that TOE users can be assigned
	  ○ System Administrator
	  ○ Account Owner
	  ○ Manager
	  ○ Operator
	• Security attributes determine the TOE functionalities and access to data that are available to TOE users.
	• TOE users with the appropriate roles (Managers, Account Owners, System Administrators) are privileged to create other TOE users using the User Account Creation function.
	• TOE users with the appropriate roles (Managers, Account Owners) are privileged to change passwords of other users within their accounts using the Change Password function.
	• TOE users with the appropriate roles (Managers, Account Owners) are privileged to assign and unassign user roles of other TOE users.

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 segregates data accoding to an access matrix that determines what type of data and how much data can be obtained by any particular user role.

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

2.5.3 Data Management

From the perspective of data management, the TOE provides functionality to manage the four categories of data, based on the assigned role of the authenticated TOE user, as shown in the following table.

Data Category	Description	Managed By			
		Operator	Manager	Account Owner	System Administrator
Operations Data	• Officer activities, locations and statuses • Tasks • Incidents • Occurrences • Messages and broadcasts	✓	✓		
User Data	• First name • Last name • Display name • Password • Email address • Active • Assigned role • Assigned user groups • Assigned organizations • Assigned account		✓	✓	✓
Organization Data	• Task templates • Duty plans • User groups • Operations metadata • Reports		✓		
Account Data	• Organizations • Organization structure • Accounts			✓	✓

2.5.4 Deliverables to TOE Users

The Argus Preparative Team installs the Argus System in the AWS cloud hosting environment using an infrastructure provisioning tool known as AWS CloudFormation. In addition to infrastructure being provisioned, the various Argus applications, including the TOE, are also installed by the Preparative Team.

As the TOE is offered as a web-based application accessible over the Internet, there is no hardware or software installation required on the part of the TOE users. With reference to Sec. 5.2.3 of 2019 Certis Cisco – Argus CC EAL2 -Operational User Guidance [AGD_OPE.1] & Preparative Procedure [AGD_PRE.1] supporting document, the TOE is provisioned by the Argus Preparative Team and the System Administrator login credentials are configured and provided to the appointed TOE user assuming this role, with the following information.

- URL of Argus CC (the TOE)
- System Administrator username

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

- System Administrator password

For users other than the System Administrator, provisioning is based on a software-as-a-service (SaaS) model. Business units raise service requests to the System Administrator, who is responsible for creating Argus Accounts and associated Account Owner users. Account Owners can then access the TOE to manage their own Account.

The delivery process and instructions briefly mentioned in this section are provided to the TOE Users in the form of the following guidance documentation, as aforementioned in Sec. 2.5.1.

- 2019 Certis Cisco – Argus CC EAL2 -Operational User Guidance [AGD_OPE.1] & Preparative Procedure [AGD_PRE.1]
- 2019 Certis Cisco – Argus CC EAL2 – Delivery [ALC_DEL.1]

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 addressed;
- 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 between the TOE and TOE users, such that sensitive information including usernames, passwords, operations-related data (tasks, incidents) are leaked to unintended parties.
T.WEAK_PASSWORD_GENERATION	The newly generated password provided to the TOE users during Change Password process and for User Account Creation function are weak and easily brute-forced by malicious parties to gain access to the TOE's functions.

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 (username and password) where the attribute of the password consists of (at least one) uppercase, lowercase, alphanumeric, special characters and a minimum length of 10 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.

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

	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.

5.3 ASSUMPTIONS

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

Assumption Identifier	Assumption Statement
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 willfully 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.
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.

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 or functions 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 minimize likelihood of illicit access through methods such as brute force attempts and login bypasses made by arbitrary individuals, the TOE shall employ the following security mechanisms. a. Impose password complexity to increase difficulty of guessing passwords, whether the passwords are generated by the system or specified by TOE users. b. Limit failed authentication attempts to block brute force attacks. SPD Mapping Threat: T.BROKEN_AUTH OSP: P.PASSWORD
O.SEC_COMMUNICATION	Objective Statement The TOE shall ensure that communication channels are secure by ensuring that only the TLS 1.2 and above protocols, including secure cipher suites and algorithms, are used when establishing HTTPS connections between the TOE and the Argus System. SPD Mapping Threat: T.INTERCEPTION OSP: P.CRYPTO
O.SEC_PASSWORD_GENERATION	Objective Statement The TOE shall ensure that a randomly secured password will be generated for the following scenarios: a. User account creation b. Change Password function initiated by Managers and Account Owners SPD Mapping Threat: T.WEAK_PASSWORD_GENERATION OSP: P.PASSWORD

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

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 System Administrator who manages the TOE is non-hostile, competent and applies all administrative guidance in a trusted manner. SPD Mapping Assumption: A.TRUSTED_ADMIN
OE.DEVELOPER	Objective Statement The owners of the TOE must ensure that the developers who built the TOE are non-hostile, trustworthy individuals and competent with suitable training provided. SPD Mapping Assumption: A.TRUSTED_DEV
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_CLOUD	Objective Statement The TOE must be installed and operated in a physically secured area. The TOE is operated without any discrepancies by the trustworthy cloud service provider. SPD Mapping Assumption: A.CLOUD
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.SAFE_CONNECTIVITY	Objective Statement The TOE uses a trusted and secure Internet connection.

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

	SPD Mapping Assumption: A.CONNECTIVITY
OE.THIRDPARTY	Objectve Statement The TOE accepts all integrated third-party data that maintains its integrity and nonrepudiation. SPD Mapping Assumption: A.THIRDPARTY

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**	**T.WEAK_PASSWORD_GENERATION**	**P.ACCESS_ROLE**	**P.PASSWORD**	**P.CRYPTO**	**A.TRUSTED_ADMIN**	**A.TRUSTED_DEV**	**A.TIMESTAMP**	**A.CLOUD**	**A.MALWARE**	**A.DDOS**	**A.CONNECTIVITY**	**A.THIRDPARTY**
O.SEC_ACCESS		✓			✓										
O.SEC_AUTHENTICATE	✓					✓									
O.SEC_COMMUNICATION			✓				✓								
O.SEC_PASSWORD_GENERATION				✓		✓									
OE.ADMINISTRATOR								✓							
OE.DEVELOPER									✓						
OE.SYN_TIMESTAMP										✓					
OE.SAFE_CLOUD											✓				
OE.ANTI_MALWARE												✓			
OE.ANTI_DDOS													✓		

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

OE.SAFE_CONNECTIVITY													✓	
OE.THIRDPARTY														✓

✓ 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 System Administrator and TOE Manager to access TOE configuration data and manage master data functions. The security objective also ensures that any TOE user will be denied access when attempting to enter/use a function where the user has not been assigned the privilege. For example, Operators cannot access the Manager Portal or its functions and Managers cannot access the Account Owner Portal.
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.
T.WEAK_PASSWORD_GENERATION	O.SEC_PASSWORD_GENERATION	The security objective ensures that the password defined during Manager / Account Owner initiated password change and provided for TOE user creation is using a combination of secured and randomly generated characters which increases password complexity.

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 access to TOE functions based on the individual role assigned to TOE users, such as Operator, Manager, Account Owner and System Administrator. Managers can create users and assign them the Operator role in the Manager Portal. Account Owners use the Account Owner Portal to create Managers and Operators. The System Administrator creates Accounts and the Account Owners that belong to the Accounts.

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

P.PASSWORD	O.SEC_AUTHENTICATE O.SEC_PASSWORD_GENERATION	The security objective ensures that the OSP is satisfied by implementing and enforcing secure password policies. When passwords are generated by the system, for example by the Change Password function, the generated passwords must also follow the password complexity policy in-force.
P.CRYPTO	O.SEC_COMMUNICATION	The security objective ensures that the OSP is satisfied by the usage of TLSv1.2 and above and the enforcement of secure communications protocol and secure cipher suites and algorithms.

6.3.4 Rationale for Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
A.TRUSTED_ADMIN	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.TRUSTED_DEV	OE.DEVELOPER	The security objective counters this assumption that those responsible for the TOE's development and deployment are competent and trustworthy individuals, capable of building the TOE appropriately, maintaining the security and configuration of the TOE and information within.
A.TIMESTAMP	OE.SYN_TIMESTAMP	The security objective counters this assumption because the TOE environment provides reliable, accurate and synchronized timestamps.
A.CLOUD	OE.SAFE_CLOUD	The security objective counters this assumption because the TOE and its environment shall be physically secure within the cloud hosting. Cloud service providers are competent and trustworthy individuals, capable of refraining from tempering or accessing the TOE's contents.
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.CONNECTIVITY	OE.SAFE_CONNECTIVITY	The security objective counters this assumption because the TOE shall use a trusted and secure Internet connection.
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.

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 failure 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_SOS.2	TSF Generation of secrets	No dependencies
FIA_UAU: User Authentication		
FIA_UAU.1	Timing of authentication	FIA_UID.1 Timing of identification
FIA_UID: User Identification		
FIA_UID.1	Timing of identification	No dependencies
CLASS FMT: SECURITY MANAGEMENT		
FMT_MSA: Management of Security Attributes		
FMT_MSA.1	Management of security attributes	FDP_ACC.1 Subset access control FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.3	Static attribute initialisation	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_SMF: Specification of Management Functions		
FMT_SMF.1	Specification of Management Functions	No dependencies
FMT_SMR: Security Management Roles		
FMT_SMR.1	Security roles	FIA_UID.1 Timing of identification
CLASS FTP: TRUSTED PATH/CHANNELS		
FTP_ITC: Inter-TSF Trusted Channel		
FTP_ITC.1	Inter-TSF trusted channel	No dependencies
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

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 [**ten (10)**] 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 [**lock out the user account for 30 minutes, and notify the user that his account has been locked out through his registered email address**].
Application Note(s):	This requirement defines the action and behavior of the TOE when handling authentication failures during the user authentication process.

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) User identity: username** **b) Passphrase: password** **c) Authorization:** **i. roles** **ii. assigned account** **iii. assigned organizations** **d) User registration: email address** **e) Active**].
Application Note(s):	This requirement stipulates the security attributes that enforce authentication for users and govern the authorization of user access to TOE functions. The “Active” boolean attribute denotes whether a TOE user is allowed to sign in or not (“true” means active and allowed to sign in, “false” means not active and not allowed to sign in.)

7.1.3 FIA_SOS: Specification of Secrets

FIA_SOS.1 Verification of Secrets	
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [**a) at least 10 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, first-time login and change of password. TOE users can change their passwords using two methods.

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

	The first is a self-service method ("Forgot your password?" function) where TOE users can request for a reset password link to be emailed to their registered email address on the TOE login page. The user's password is not changed by the TOE until the user visits the reset password page to change his/her password. The second method is meant for TOE users with the appropriate permissions (Managers, Account Owners) to change the TOE users' passwords immediately, which the TOE will then generate a random password, in accordance to the password complexity rules, and email the users with the temporary password. Users logging in with the temporary password will have to change their password.

FIA_SOS.2 TSF Generation of Secrets	
FIA_SOS.2.1	The TSF shall provide a mechanism to generate secrets that meet [**a) at least 10 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)**].
FIA_SOS.2.2	The TSF shall be able to enforce the use of TSF generated secrets for [**a) User Account Creation function and** **b) Change Password function**].
Application Note(s):	Random temporary passwords are created based on the stipulated password complexity rules for newly created user accounts. For first-time logins, TOE users who use the randomly generated temporary passwords will be redirected to change their passwords. Managers and Account Owners are privileged to use the Change Password function on users within their accounts.

7.1.4 FIA_UAU: User Authentication

FIA_UAU.1 Timing of Authentication	
FIA_UAU.1.1	The TSF shall allow [**a) "Forgot your password?" function (Security Management) and** **b) Account Lockdown function (Identification and Authentication)**] 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):	TOE users can use the self-service reset password ("Forgot your password?" function) available on the TOE login page to request for a reset password link that will be emailed to their registered email address. The TOE does not change the user's password yet. The link directs the user to the reset password page where the user is able to update his/her password. The Account Lockdown function tracks unsuccessful authentication attempts (more than 10) and disables a user's account when the threshold has been breached. This function ensures that unauthorized parties cannot perform brute force authentication.

7.1.5 FIA_UID: User Identification

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

FIA_UID.1 Timing of Identification	
FIA_UID.1.1	The TSF shall allow [**a) "Forgot your password?" function (Security Management) and** **b) Account Lockdown function (Identification and Authentication)**] 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):	TOE users can use the self-service reset password ("Forgot your password?" function) available on the TOE login page to request for a reset password link that will be emailed to their registered email address. The TOE does not change the user's password yet. The link directs the user to the reset password page where the user is able to update his/her password. The Account Lockdown function tracks unsuccessful authentication attempts (more than 10) and disables a user's account when the threshold has been breached. This function ensures that unauthorized parties cannot perform brute force authentication. No form of identification is taken place when these functions mentioned above are executed.

7.2 CLASS FMT: SECURITY MANAGEMENT

7.2.1 FMT_MSA: Management of Security Attributes

FMT_MSA.1 Management of Security Attributes	
FMT_MSA.1.1	The TSF shall enforce the [**Role-Based Access Control**] to restrict the ability to [**query, modify and delete**] the security attributes [**username, password, email address, roles, assigned account and assigned organizations**] to [**Account Owners and Managers**].
Application Note(s):	TOE verifies user identities and assigned roles before carrying out requested actions. System Administrators are privileged to modify Account Owners of any account. Account Owners are only permitted to modify users within their own accounts. Managers are permitted to modify users within their assigned organizations within their accounts.

FMT_MSA.3 Static Attribute Initialisation	
FMT_MSA.3.1	The TSF shall enforce the [**Role-Based Access Control**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**Account Owners and Managers**] to specify alternative initial values to override the default values when an object or information is created.
Application Note(s):	Users created are assigned the default role of Officer. Privileged TOE users are able to change this default role during user creation.

7.2.3 FMT_SMF: Specification of Management Functions

FMT_SMF.1 Specification of Management Functions	
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) Change user password** **b) Modify email address** **c) Create user within account** **d) Suspend user**

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

	e) Assign / unassign roles **f) Assign / unassign user to organizations** **g) Create and modify accounts**].
Application Note(s):	This requirement lists the management functions that can be used by authorized users to manage the security attributes of other users.

7.2.4 FMT_SMR: Security Management Roles

FMT_SMR.1 Security Roles	
FMT_SMR.1.1	The TSF shall maintain the roles [**a) System Administrator** **b) Account Owner** **c) Manager** **d) Operator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Application Note(s):	1) SYSTEM ADMINISTRATOR role allows users to the Account Management module of the TOE. The primary responsibilities are to modify the configuration of the TOE and to manage the creation / modification of accounts, not the management of accounts themselves. 2) ACCOUNT OWNER role allows users to access all modules within an Account. This role cannot create other Accounts. Users cannot assign other users with this role. This role is used to manage users and organizations within the account. 3) MANAGER role allows users to access all modules within an Account, except for the Account Configuration module, and confined only to the assigned organizations. 4) OPERATOR role allows users to access only operations modules of the TOE, and cannot access the Organization Configuration module.

7.3 CLASS FTP: TRUSTED PATH/CHANNELS

7.3.1 FTP_ITC: Inter-TSF Trusted Channel

FTP_ITC.1 Inter-TSF Trusted Channel	
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [**another trusted IT product**] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [**the transfer of media objects (images, videos) used by task and incident related actions**].
Application Note(s):	The TOE relies on Amazon Simple Storage Service (S3) for storage of media content, using S3 commands such as GetObject and PutObject, which can only be performed by authenticated users using a token exchange mechanism.

7.3.2 FTP_TRP: Trusted Path

FTP_TRP.1 Trusted Path

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

FTP_TRP.1.1	The TSF shall provide a communication path between itself and [**remote**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**modification and disclosure**].
FTP_TRP.1.2	The TSF shall permit [**remote users**] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [**ALL functions provided by the TOE**].
Application Note(s):	This requirement defines the communication protocol and encryption method used to protect the transmission of data between the TOE and the TOE users.

7.4 CLASS FDP: USER DATA PROTECTION

7.4.1 FDP_ACC: Access Control Policy

FDP_ACC.1 Subset Access Control	
FDP_ACC.1.1	The TSF shall enforce the [**Role-Based Access Control**] on [**Subjects:** **a) Authenticated and authorized users** **Objects:** **a) Operations data (see Sec. 2.5.3)** **b) User data (see Sec. 2.5.3)** **c) Organization data (see Sec. 2.5.3)** **d) Account data (see Sec. 2.5.3)** **Operations:** **a) Access to Operator Console (officer monitoring, task monitoring, incident response, occurrence reporting)** **b) Access to Manager Portal** **c) Access to Account Manager Portal** **d) Create users** **e) Suspend users (modify the "Active" attribute)** **f) Change password** **g) Modify email address** **h) Assign roles** **i) Assign account** **j) Assign organizations** **k) Access to Administrator Console**].
Application Note(s):	This requirement lists the subjects, objects and operations to be enforced based on the role-based access control matrix, correlated in the table below.

Objects	**Operations**										
	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)
Operations data	✓										
User data		✓		✓	✓	✓	✓	✓			
Organization data		✓									
Account data			✓						✓	✓	✓

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

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**] to objects based on the following: [**Subjects:** **a) Authenticated and authorized users** **Objects:** **a) Operations data (see Sec. 2.5.3)** **b) User data (see Sec. 2.5.3)** **c) Organization data (see Sec. 2.5.3)** **d) Account data (see Sec. 2.5.3)** **Security Attributes:** **a) Roles** **b) Active** **c) Assigned account** **d) Assigned organizations**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a) Each subject is attached to the subject's assigned role after authentication.** **b) The role, assigned account and assigned organizations are checked before any operation on the controlled objects.** **c) Access to the Operator Console requires either the Operator or Manager role.** **d) Operators and Managers are only allowed to fetch operations data based on their assigned organizations (one or more).** **e) Access to the Manager Portal requires the Manager role.** **f) Managers are only allowed to fetch user data and organization data based on their assigned organizations (one or more).** **g) Access to the Account Owner Portal requires the Account Owner role.** **h) Account Owners are only allowed to manage users and organizations within their account.** **i) Access to the Administrator Console requires the System Administrator role.** **j) System Administrators manage accounts in the Argus System.**].
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) 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 username, password and assigned account or organizations before they are authorized to perform their permitted actions.

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.
	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.
	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.
	FMT_MSA.1	This SFR will ensure only System Administrators, Account Owners and Managers are allowed to access and manage the security attributes data.
	FMT_MSA.3	This SFR will ensure only permitted users are allowed to access the TOE function and change security attribute defaults based on the assigned role.
	FMT_SMF.1	This SFR defines the management functionality.
	FMT_SMR.1	This SFR defines the relationship between the TOE's users and the associated roles respectively.
O.SEC_AUTHENTICATE	FIA_AFL.1	This SFR will handle unsuccessful authentication attempts and lock out the user account for 30 minutes if the continuous failure attempt is more than 10 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 username and password combination must be met before user is authenticated.
O.SEC_COMMUNICATION	FTP_TRP.1	This SFR provides secured and encrypted communication for data transfer between the TOE users and the TOE.
	FTP_ITC.1	This SFR provides a secure communication between the TOE and other trusted third-party applications/software end points and maintains integrity.
O.SEC_PASSWORD_GENERATION	FIA_SOS.1	This SFR will ensure user's password complexity is met.
	FIA_SOS.2	This SFR will ensure that the newly requested password during Change Password process and for User Account Creation function is generated randomly and securely.

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

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_SOS.2	No dependencies	-	-
FIA_UAU.1	FIA_UID.1	Yes	-
FIA_UID.1	No dependencies	-	-
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes	-
FMT_SMF.1	No dependencies	Yes	-
FMT_SMR.1	FIA_UID.1	Yes	-
FTP_ITC.1	No dependencies	Yes	-
FTP_TRP.1	No dependencies	Yes	-
FDP_ACC.1	FDP_ACF.1	Yes	-
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes	-

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, without any addition. The assurance components are summarized in the following table which is drawn from Part 3 of the Common Criteria.

Assurance Class	Assurance Component	Details
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	TOE design (Basic design)
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle Support	ALC_CMC.2	CM capabilities (Use of a Configuration Management system)
	ALC_CMS.2	CM scope (Parts of the TOE Configuration Management coverage)
	ALC_DEL.1	Delivery procedures
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Coverage (Evidence of coverage)
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

8.1 SECURITY ASSURANCE REQUIREMENTS RATIONALE

EAL2 was selected as the assurance level because the TOE is an internal corporate application that is not available to an audience outside of the organization, and is operated in a controlled environment with good physical access security and trusted, competent users. The chosen assurance level is consistent with the claimed threats and environment, and is sufficient to demonstrate that the TOE is resistant to attackers with a basic attack potential.

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:

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

9.2 IDENTIFICATION AND AUTHENTICATION

The TOE enforces authentication and identification of users before they can perform any action within the TOE. The only exception is the self-service reset password ("Forgot your password?" function found as a link within the login page of the TOE) feature, which only requires the TOE users to identify themselves.

All TOE users will require authentication from the TOE through the matching security attributes username, password and assigned account or organizations before they are authorized to perform their permitted actions.

The TOE requires a subset of security attributes for authentication:

i. Username
ii. Password
iii. Assigned account
iv. Active

Users are required to specify their individual password that must comply with the Company's mandated password complexity policy. Passwords must fulfil ALL of the following criteria.

i. At least ten (10) characters long
ii. At least 1 uppercase character (A-Z)
iii. At least 1 lowercase character (a-z)
iv. At least 1 digit (0-9)
v. At least 1 special character [<space>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~)] (extended ASCII codes are not allowed)

Users of the TOE are allowed to change their own password after authentication. Prior to authentication, users are able to initiate the reset password process ("Forgot your password?" function).

Account Owners and Managers are privileged to modify user passwords by utilizing the Change Password function. The function generates a random temporary password which must be changed when the TOE user logs in using that password.

The TOE does not permit modification of the password complexity policy.

Authentication attempts are monitored and controlled by the TOE. Ten (10) consecutive failed authentication attempts will lock out the offending account for thirty (30) minutes. The TOE will also notify the user of the locked account about the authentication failure.

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

Both the "Forgot your password?" function and the Account Lockdown function can be executed before the TOE users are successfully identified with their respective roles.

Summary of Security Functional Requirements Satisfied

Class Family	Property / Behavior of TSF
FIA_AFL.1	Consecutive authentication failures will cause the unauthenticated user to be locked out temporarily
FIA_ATD.1	Subset of security attributes of TOE users are maintained and enforced for authentication
FIA_SOS.1	Enforcement of password complexity rules
FIA_SOS.2	System-generated passwords comply to password complexity rules
FIA_UAU.1	Unauthenticated users are restricted to the primary functions of the TOE except for the "Forgot Password" and "Account Lockdown" functions.
FIA_UID.1	Unidentified users are restricted to the primary functions of the TOE except for the "Forgot Password" and "Account Lockdown" functions.

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

9.3 SECURITY MANAGEMENT

The TOE stipulates a fixed set of Roles that determines the access level of every TOE user and his or her access to specific TOE functional modules. The Roles are as follows.

i. System Administrator
ii. Account Owner
iii. Manager
iv. Operator

The user interface provided by the TOE allows System Administrators, Account Owners and Managers to manage the security attributes of TOE users. The TOE maintains the following list of security attributes belonging to individual users:

i. Username
ii. Password
iii. Email address
iv. Roles
v. Active
vi. Assigned account
vii. Assigned organizations

Except for System Administrators, every TOE user (with Account Owner, Manager and Operator roles) belongs to an Account. This enables the TOE to provide multi-tenancy functionality and segregation of user data. Within an Account, every TOE user can be assigned to one or more Organizations. As System Administrators do not belong to any Account, they cannot access modules that require users to be assigned to an Account, such as the Operations, Organization Management and Account Configuration modules mentioned in Section 9.5 USER DATA PROTECTION.

By default, a newly created TOE user is assigned only the Officer role and the default role can be changed by Account Owners and Managers during user creation. Only Account Owners and Managers are permitted to add or remove roles from TOE users after user creation. These roles are ordered by permissiveness, with System Administrators having the most permissions, Account Owners having permissions to manage their accounts, and Managers who are restricted to managing only users within their assigned organizations. Based on this order, more restrictive roles cannot manage higher level roles, e.g. Managers cannot modify users having the Account Owner role.

Users of the TOE assigned with the Operator role are permitted to access only the Operations modules of the TOE, but not the administrative modules, which comprise the Account Management, Account Configuration and Organization Management modules.

The TSF is capable of performing the following management functions:

i. Change user password
ii. Modify email address
iii. Create user within account
iv. Suspend user
v. Assign / unassign roles
vi. Assign / unassign user to organizations
vii. Create and modify accounts

Summary of Security Functional Requirements Satisfied

Class Family	Property / Behavior of TSF

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

FMT_MSA.1	Role-Based Access Control is enforced using User Roles to restrict the ability to query, modify and delete security attributes of TOE users
FMT_MSA.3	Account Owners and Managers are privileged to modify initial default values of security attributes
FMT_SMF.1	TOE provides management functions to privileged users (based on roles) to manage security attributes of other users
FMT_SMR.1	TOE users can be assigned different user roles to enable or restrict their access to TOE functionality

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

9.4 TRUSTED PATH/CHANNELS

The TOE user interface provides web-based access to its functions through web browsers. The TOE strictly enforces secure communication with the Argus System (non-supporting TOE components) using the HTTPS/TLS protocol, maintaining the confidentiality and integrity of data transmission between both systems. Furthermore, the TOE does not support unencrypted communication with the Argus System, simply due to the fact that the Argus System does not accept or process data transmitted over any unencrypted HTTP channel.

The TOE also enforces secure resource loading for its runtime environment through the usage of web server directives, such as HTTP Strict-Transport-Security. Compliant environments (web browsers) will reject requests for resources if they are unencrypted, whether from the TOE's originating domain or third-party websites.
Operations modules, such as the incident reporting module, interact with third-party services, such as Amazon Simple Storage Service (S3) for functions such as uploading and downloading of images. All communication with S3 is encrypted using HTTPS/TLS protocol. Additionally, all communicated requests with S3 have to be authenticated using tokens that the TOE requests from AWS Security Token Service (STS). STS issues temporary, limited privilege credentials that are used to interact with AWS resources, such as S3.

Summary of Security Functional Requirements Satisfied

Class Family	Property / Behavior of TSF
FTP_ITC.1	Only secure connections are established to Amazon Simple Storage Service (S3) for the purpose of transferring media objects such by task and incident relation actions.
FTP_TRP.1	Secure communication is achieved by establishing encrypted channels from the TOE to the Argus System, using HTTPS (TLS 1.2).

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

9.5 USER DATA PROTECTION

The TOE employs Role-Based Access Control (RBAC) to differentiate user roles and responsibilities and segregate user data according to the following role-based matrix that determines the type of operations any particular role is privileged to perform.

Role	Module			
	Operator Console	Manager Portal	Account Owner Portal	Administrator Console
System Administrator				✓
Account Owner			✓	
Manager	✓	✓		
Operator	✓			

The functions within each module is listed as follows.

Module	Functions	Description
Operator Console	• Task assignment and monitoring • Incident response • User monitoring • Messaging • Occurrence book • Report generation	These functions are used by TOE users who are assigned the Operator role to manage and monitor the security operations supported by the Argus System. This module can also be utilized by TOE users assigned the Manager and Account Owner roles even though the usage of the Operations module is not their primary responsibility. The functionalities within this module are the same for the different TOE user roles.

Manager Portal	• User management
	  ○ Create, modify users
	  ○ Change password
	  ○ Change user roles
	• Task Planner
	• Data management
	• Report generation
		These functions allow Managers to modify the users and tasks within their assigned Organizations.
		
		This module can also be utilized by TOE users assigned the Account Owner role, perhaps in cases where the TOE users do not deem the need to delegate the management of their Organizations to other less privileged users, i.e. Manager roles.

Account Owner Portal	• User management
	  ○ Create, modify users
	  ○ Change password
	  ○ Change user roles
	  ○ Assign organizations
	• Organization management
	  ○ Create, modify organizations
		These functions are used by Account Owners to manage the hierarchical structure of Organizations within their Accounts, by creating and modifying Organizations. Account Owners also manage the users within each of their Account, and assign users to their respective Organizations.

Administrator Console	• Create, modify accounts • Create and assign Account Owners	System Administrators use these functions to create Accounts and to create Account Owners that are associated to the Accounts.

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

After authentication, users of the TOE are privileged to access the modules and perform the functions that are permitted by their assigned roles. Each user can only be assigned ONE role.

The TOE provides a multi-tenant operating model that segregates user data into independent Accounts. With the exception of System Administrators, TOE users can only access user data and perform related operations within their assigned accounts. Each user can only be assigned to ONE account.

Within an account, the RBAC policy is combined with a hierarchical access control policy to determine the Organizations where users can perform related operations. An account consists of an Organization structure that is hierarchical in nature. The Account Owner role is not confined by this structure. Only the Manager and Operator roles are tied to Organizations. A TOE user with the Operator role can access the Operations modules for his assigned Organization and every child / descendant Organization belonging to the assigned TOE user. Similarly, a TOE user with the Manager role can access not only the Operations modules, but also the Organization Configuration module of the Organization that he has been assigned to, including every other child / descendant Organization. In effect, this means that Managers can only modify the user data (security attributes) of TOE users that are assigned to his "tree" of Organizations.

Summary of Security Functional Requirements Satisfied

Class Family	Property / Behavior of TSF
FDP_ACC.1	Role-Based Access Control is enforced to ensure that privileged TOE users access only the permitted subset of data.
FDP_ACF.1	Role-Based Access Control, complemented by assignment of Organizations and Accounts, ensures that TOE users access only the functions available to their particular role and that the data available to them is confined to their assigned Organizations and Account.

[End of Document]

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