RADMIK SOLUTION
Reinventing Technology

Radmik Solution RADIUSS Core EAL1 Security Target

Version 1.1

9-JULY-2012

Document management

Document identification

Document ID	RAD_EAL1_ST
Document title	Radmik Solution RADIUSS Core EAL1 Security Target
Product version	2.0

Document history

Version	Date	Description
0.1	01-MAY-10	Release for internal review.
0.2	18-APR-11	Addressing ASE EORs v1.0
0.3	15-AUG-11	Updating security objective for the environment.
1.0	15-SEP-11	Release for MyCB review
1.1	9-JULY-12	Addressing CAR - ISCB-3-CAR-C024-CAR_003-v1

Table of Contents

1 Security Target introduction (ASE_INT)

1.1 ST and TOE identification

ST Title	Radmik Solution RADIUSS Core EAL1 Security Target
ST Version	1.1, 9-JULY-2012
TOE	RADIUSS Core
TOE Version	2.0
Assurance Level	EAL1
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, July 2009, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009; • Part Two – Security Functional Components, Revision Three, July 2009; and • Part Three – Security Assurance Components, Revision Three, July 2009. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004

1.2 Document organization

This document is organized into the following sections:

- Section 1 provides the introductory material for the ST as well as the TOE description including the physical and logical scope of the TOE.
- Section 2 provides the conformance claims for the evaluation.
- Section 3 defines the security objectives for the environment.
- Section 4 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.

- Section 5 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE

1.3 TOE description

1.3.1 TOE type and usage

The Target of Evaluation (TOE) is RADIUSS Core. RADIUSS Core (Radmik Intelligent Universal Surveillance System) is a management IP based solution for CCTV system that connect directly to preferred network and is manageable remotely via local area network or the Internet.

RADIUSS Core easily handles simultaneous recording and remote access to live views and playback of recorded videos, with hybrid support for a large number of IP cameras and analogue video sources. RADIUSS Core has been designed to be a reliable solution offering high-availability and load-balancing when using multiple servers.

RADIUSS Core is part of the RADIUSS framework. The TOE is a Java software module designed to be used as core security module that provide security functionality such as identification and authentication of administrators and its users, managing security logs for auditing purpose, and security management of the cameras.

RADIUSS Core also has features that enable RADIUSS to do these functionalities, such as:

- Record video from cameras
- Re-stream video from cameras to clients
- Monitor camera status
- Storage cleaning
- Centralized license management
- Manage connection to database (local and centrals)

All RADIUSS Core features are accessible through RADIUSS Clients Graphical User Interface that are installed in a user terminal which consists of RADIUSS Skrin, RADIUSS Configurator and RADIUSS CMS (Centralized Monitoring System). Every request by these RADIUSS Clients will be processed by RADIUSS Core before the RADIUSS Clients gets the feedback.

1.3.2 TOE security functions

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

Security function	Description
Auditing	The TOE generates logs for video feeds (time when recording start, IP address of cameras, motion detection and other information) and for users (success/failure of user authentication, change of passwords for users and other information). Upon detection of a movements from motion detection cameras, an alert can be sent and trigger an SMS/email to be sent to users.
Access Control	User data (video feeds, logs) can be viewed by authorized users. Administrator can configure the access to functionalities and data for each role that is allocated to users.
Identification and authentication	Administrators and users will need to identify and authenticate themselves before allowing TSF-mediated actions.
Security Management	Administrators are able to execute security management functions through the web interface provided by the TOE. The management functions include: • User management • Log management • ACL (Access Control List) Management • Video camera management

1.3.3 Supporting hardware, software and/or firmware

Before the TOE can be installed in a working environment, it needs to fulfill some pre-requisites that have to be met. Those pre-requisites include hardware and software. Below is the minimum requirement for the hardware and software:

a. Hardware requirement:

1. Any Intel Core 2 Duo processor
2. 1GB of RAM

3. 1 x 100 Mbps LAN port

4. 100GB of storage

b. Software requirement:

1. Operating system supporting Java 1.6 (i.e. SuSE, Red Hat, CentOS, Ubuntu)

2. A web server with PHP5 module installed (i.e. Apache 2.0)

3. MySQL 5

4. Monit

5. VLC 0.9

1.4 Physical scope of the TOE

The TOE is RADIUSS Core which is part of RADIUSS Core framework. A typical installation of the TOE can be found in Figure 1 below and identifies the various roles and components of the RADIUSS.

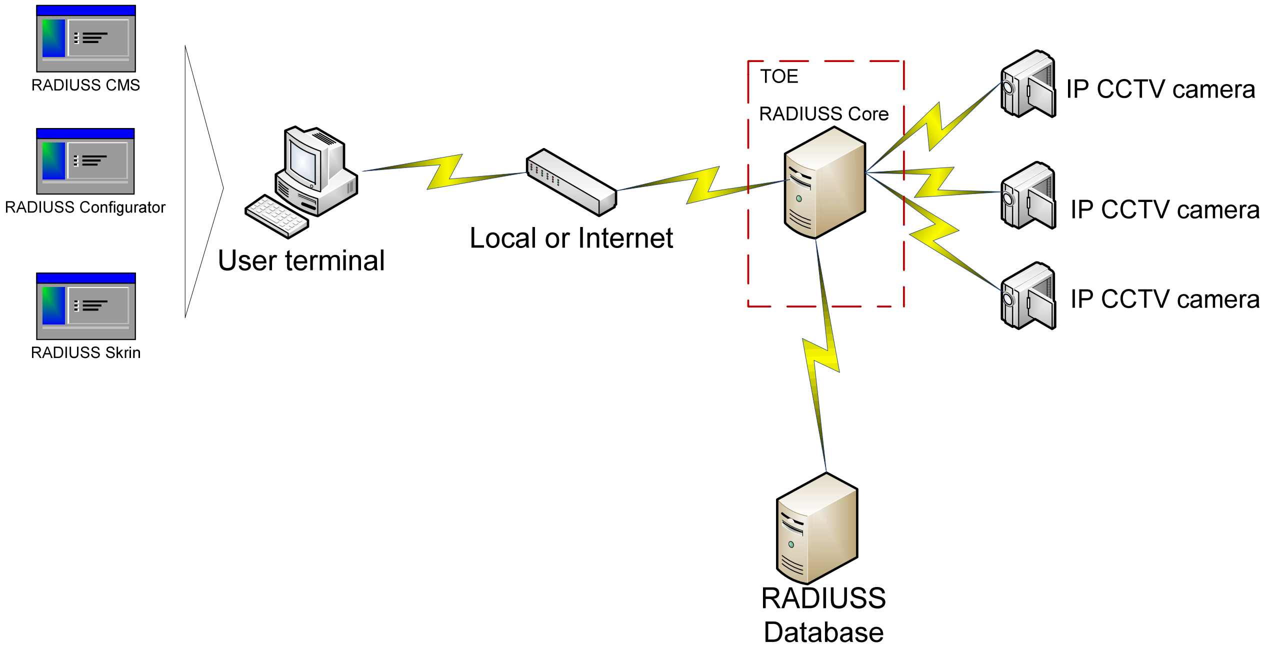

Figure 1 – RADIUSS Core Deployment

The following table describes each of the RADIUSS components specified in Figure 1 above.

Component role	Description
RADIUSS Core (TOE)	The TOE itself which is part of the RADIUSS framework. It provides core security functionalities for RADIUSS.
IP CCTV camera	CCTV camera with IP based in which that it is being used to record or monitor a specific location.
RADIUSS Database	RADIUSS Database is used to store user information, stores video feeds database from the camera, and other information needed by RADIUSS.
User terminal	Authorized user that can access the RADIUSS Core from several GUI interfaces (RADIUSS Clients) that interact with RADIUSS Core.

1.5 Logical scope of the TOE

The logical boundaries of the TOE include the functions of the TOE interfaces. These functions include audit, identification and authentication, security management, and intrusion detection.

Audit

The TOE generates audit data that comprises security relevant events such as user logging, camera service interruptions, video feeds accessed, and other information which are further described in section 5.1.1. Upon detection of a intrusion by motion-sensor cameras, the TOE will send an alert to the other components of RADIUSS Core.

Access Control

User data (video feeds, logs) can only be viewed by authorized users. Users will have to identify and authenticate themselves and will be allocated a pre-defined role set by the administrator. Depending on their roles and user ID, they can only view the video feeds of those cameras that are allocated to them.

Identification & Authentication

The TOE requires users to provide unique identification and authentication data before any administrative access to the TOE is granted. The TOE provides an authentication mechanism for users through a web interface. The only authentication mechanism supported by the TOE is passwords. Refer to 5.1.3 for detailed information.

Security Management

The TOE provides the authorized users to administrative functions. There are several modules available to the authorized users of the TOE, such as modify the behavior of the data collection and review, query audit data, and restrict access and/or the ability to query and modify all other TOE data to the appropriate authorized user/authorized role. Refer to 5.1.4 Security Management for detailed information.

2 Conformance Claim (ASE_CCL)

The ST and TOE are conformant to version 3.1 (Revision 3) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, July 2009.
- Part 3 conformant, EAL1. Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3. Evaluation is EAL1.

3 Security objectives (ASE_OBJ)

3.1.1 Overview

The security objectives at an EAL1 level of assurance include concise statements of the objectives to be achieved by the supporting environment.

3.1.2 Security objectives for the environment

Identifier	Objective statements
OE.AUDIT	The IT Environment will provide the capability to protect audit information.
OE.TIME	The IT environment will provide reliable timestamps to the TOE.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE. CREDENTIALS	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.ADMIN	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
OE.NETWORK	Those responsible for TOE must configure the TOE to use secure channel for the network between the TOE and other components.

4 Security requirements (ASE_REQ)

4.1.1 Overview

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

4.1.2 SFR conventions

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

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

4.2 Security functional requirements

4.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 4.1.2 and summarized in the table below.

Identifier	Title
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1	Potential violation analysis
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles

4.2.2 FAU_ARP.1 Security alarms

Hierarchical to:	No other components.
FAU_ARP.1.1	The TSF shall ~~take~~ [**send an alert to the Authorized Users**] upon detection of a potential security violation.
Dependencies:	FAU_SAA.1 Potential violation analysis
Notes:	None.

4.2.3 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [***not specified***] level of audit; and c) [**the following auditable events:** **a) user identification and authentication** **b) Receiving of camera feeds and data** **c) User management** **d) Video device management** **e) Motion detect by motion sensor camera**].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**date, time, camera's IP, user ID**].
Dependencies:	FPT_STM.1 Reliable time stamps
Notes:	None.

4.2.4 FAU_GEN.2 User identity association

Hierarchical to:	No other components.

FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
Notes:	None.

4.2.5 FAU_SAA.1 Potential violation analysis

Hierarchical to:	No other components.
FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [**motion detected by motion sensor camera**] known to indicate a potential security violation; b) [**None**].
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

4.2.6 FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**MD5**] and cryptographic key sizes [**none**] that meet the following: [**FIPS 180-2**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	This cryptographic operation does not use key. The password of the users is hashed and compare with the values stored in the database.

4.2.7 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**User Access Control SFP**] on [**Subjects:** a) **User, Administrator** **Objects:** a) **Video Feeds** **Operations:** a) **Viewing of video feeds**]**.**
Dependencies:	FDP_ACF.1 - Security attribute based access control
Notes:	None.

4.2.8 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**User Access Control SFP**] to objects based on the following: [**Subject attribute:** a) **ID of the user** b) **corresponding user role** **Object attributes:** a) **Access Control List**].
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) **The Access Control List for an object permits the user ID to access that object; OR** b) **The Access Control List for an object permits the User Role to access that Object**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**the Administrator role can access all records and functions**].

FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

4.2.9 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**a) User ID** **b) Role** **c) Password**].
Dependencies:	No dependencies.
Notes:	None.

4.2.10 FIA_UAU.2User authentication before any action

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

4.2.11 FIA_UID.2User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.

Notes:	None.

4.2.12 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**User Access Control SFP**] to restrict the ability to [***delete, [***write***]***] the security attributes [**that map user IDs to roles to only the users that are mapped**] to [**administrator**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

4.2.13 FMT_MSA.3 Static attribute initialisation

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

4.2.14 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) mapping user IDs to roles** **b) creation of users with default passwords** **c) enrolment of new camera**

	d) deletion of users **e) deletion of camera** **f) changing of passwords** **g) management of Access Control lists** **h) log management**]
Dependencies:	No dependencies.
Notes:	None.

4.2.15 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**custom user and administrator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3 Dependency analysis

SFR	Dependency	Inclusion
FAU_ARP.1	FAU_SAA.1 Potential violation analysis	FAU_SAA.1
FAU_GEN.1	FPT_STM.1 Reliable time stamps	TOE receives data from several IP CCTV cameras hence there will be issues if TOE provide time stamp for every event. Thus, TOE takes the timestamp from NTP server (IT Environment) and this SFR is not applicable.
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1 FIA_UID.2
FAU_SAA.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FCS_COP.1	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	MD5 is a hashing algorithm and is a one way function. Therefore it does not use any key for hashing and there is no FCS_CKM.1 and FCS_CKM.4 involved for the function. Therefore the dependencies are not applicable.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3

SFR	Dependency	Inclusion
FIA_ATD.1	No dependencies	N/A.
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A.
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No dependencies.	N/A.
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2

4.4 TOE security assurance requirements

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 1 (EAL1).

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behavior.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

This EAL provides a meaningful increase in assurance over unevaluated IT.

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.1 TOE CM coverage
	ALC_CMC.1 Labelling of the TOE
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance

Assurance class	Assurance components
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

4.5 Assurance measures

Assurance requirement	Assurance measures	Demonstration
ADV_FSP.1 Basic functional specification	Development	The development assurance measure provides all the necessary design documentation to support the analysis of the TOE for an evaluation at EAL1. The functional specification provides a detailed description of the security functions of the TOE.
AGD_OPE.1 Operational user guidance	Guidance documents	The operational user guidance documentation provides the guidance for end users, administrators and other parties who will utilise the TOE. These documents provide all the necessary instructions and direction for ensuring that the TOE is installed, configured, used and administered in a secure manner.
AGD_PRE.1 Preparative procedures		
ALC_CMC.1 Labelling of the TOE	Life cycle support	Configuration management measures provide the assurance that the TOE and supporting evidence can be uniquely identified.
ALC_CMS.1 TOE CM coverage		
ASE_CCL.1 Conformance claims	Security Target evaluation	Security Target evaluation assurance measures ensure that the claim to EAL1 can be accurately appraised.
ASE_ECD.1 Extended components definition		
ASE_INT.1 ST Introduction		
ASE_OBJ.1 Security objectives for the operational environment		

Assurance requirement	Assurance measures	Demonstration
ASE_REQ.1 Stated security requirements		
ASE_TSS.1 TOE summary specification		
ATE_IND.1 Independent testing - conformance	Tests	The tests assurance measure ensures that the TOE has been appropriately tested for the claimed set of security functions. The test plans for the TOE identifies the set of security functions that are to be tested, the procedures for establishing the test environment and also for conducting the test cases. The results of the tests are also recorded to provide evidence of test results.
AVA_VAN.1 Vulnerability survey	Vulnerability assessment	The TOE will be made available for vulnerability analysis and penetration testing.

4.6 Defined Terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Term/Acronym	Definition
RADIUSS	Radmik Intelligent Universal Surveillance System
CCTV	Closed-circuit television which transmit a signal to a specific place such as a storage room in a store that are connected on a monitor. Mostly used as surveillance systems.
Motion sensor camera	A type of camera that is able to detect motion changes for example object's movement. Normally, if motion is detected, the camera will send an alarm.
NTP Server	Network Time Protocol server, a protocol that provide for synchronizing the time of computer systems in a network.

5 TOE summary specification (ASE_TSS)

5.1 Overview

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

The TOE security functions include the following:

- **Audit**
- **Access Control**
- **Identification and Authentication**
- **Security Management**

5.1.1 Audit

The TOE records two types of events; video camera-related events and user-related events. Security events relate to the proper functioning and use of the system, and allow an administrator to track the management functions performed. All the events are identified by the user ID or the capture devices IP addresses that caused the events (**FAU_GEN.1, FAU_GEN.2**).

The TOE obtains the date/timestamp from the IT environment. No security related actions can be taken without a successful user identification and authentication. The TOE allows only users who have the Administrator role to view the audit records.

Following are the events that are recorded;

- The start-up and shutdown of audit functions (the audit function automatically starts at system start-up and can only be shutdown at system shutdown. In both instances, a record is of the event is recorded.)
- Success and failure of authentication to TOE
- Motion detect by motion-sensor camera
- Access to the video feeds

- Reading of information from the audit records
- All modifications to the audit configuration that occur while the audit collection functions are operating
- All modifications to the values of TSF data
- Changing of user passwords
- Modifications to the group of users that are part of a role
- Enrollment/removing of capture devices that the TOE gets the video feeds

Upon the detection of any movements that are captured by the motion-sensor camera, the camera will send an alert to TOE and the TOE will determine to send an alert to specific user. (**FAU_SAA.1, FAU_ARP.1**).

5.1.2 Access Control

The TOE enforces an access control policy on video feeds that are stored in the database. After a user identifies and authenticates to the TOE, the TOE will check all requests to the video feeds from the user. The TOE will permit a user to access a protected resource only if a userID or role of the user has permission to view the video from a particular camera (**FDP_ACC.1, FDP_ACF.1**). The TOE maintains access control lists for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

There are 2 users maintained by the TOE. They are custom user, and Administrator (**FMT_SMR.1**). Each type of user will have different access rights to a user data and functionalities of the TOE. All users will have a unique user ID.

5.1.3 Identification and Authentication

To protect the passwords, the TOE only stores MD5 hashes of the passwords in the database. The TOE provides the graphical user interface (GUI) for administrators to create and maintain the user accounts (**FCS_COP.1**).

The following attributes are associated with the user (**FIA_ATD.1**):

- User ID
- Authentication data (passwords)

- Authorizations (roles).

The TOE requires users to provide unique identification and authentication data (passwords) before any access to the TOE is granted. Each user must be successfully authenticated; by providing the correct password associated with the user identity (**FIA_UAU.2, FIA_UID.2**).

To login to the TOE, the user provides the user ID and password. The TOE compares the password to that stored in the database. If either the login name or the password is incorrect, the login request will fail and no access to any functions will be made available. As result of a successful login, the session is established and authenticated user can access the TOE functionalities according to the role that is assigned to that particular user.

5.1.4 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE (**FMT_SMF.1**):

- **User management**
- **Log Management**
- **ACL Management**
- **Video camera management**

User management includes the creation/deletion/modification of users and assigning each user to a role. ACL (Access Control List) Management is to manage the actions that can be done by certain roles.

Log management function can be used to allow certain users to view certain event logs, while video camera management allows users to enrol/remove camera.

Only Administrator and specific custom user role can modify the access control list, mapping of users to roles, registering/removing cameras, viewing certain event logs as well as modifying the user accounts (**FMT_MSA.1**)

The TOE maintains 2 roles (**FMT_SMR.1**) within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: Custom user, and Administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

The TOE allows no one to change the default values of the TSF data and security attributes of the TOE (**FMT_MSA.3**).