Huawei Integrated Management Application Platform Security Target

Version: V0.63
Last Update: 2011-08-24
Author: Huawei Technologies Co., Ltd.

Table of Contents

HUAWEI INTEGRATED MANAGEMENT APPLICATION PLATFORM VERSION 3 RELEASE 1 ..... **1**

SECURITY TARGET **1**

TABLE OF CONTENTS **2**

LIST OF TABLES **3**

LIST OF FIGURES **3**

1 INTRODUCTION **4**

1.1 ST reference 4

1.2 Target of Evaluation（TOE）reference 4

1.3 TOE Overview 4

1.3.1 TOE usage 5

1.3.2 TOE type 5

1.3.3 Non TOE Hardware and Software 6

1.4 TOE Description 6

1.4.1 Architectural overview 6

1.4.2 Scope of Evaluation 8

1.4.3 Summary of Security Features 9

2 CC CONFORMANCE CLAIM **12**

3 TOE SECURITY PROBLEM DEFINITION **13**

3.1 Threats 13

3.1.1 Assets 13

3.1.2 Agent 13

3.1.3 Threats 14

3.2 Assumptions 14

3.2.1 Environment of use of the TOE 14

4 SECURITY OBJECTIVES **16**

4.1 Objectives for the TOE 16

4.2 Objectives for the Operational Environment 16

4.3 Security Objectives Rationale 16

4.3.1 Coverage 16

4.3.2 Sufficiency 17

5 EXTENDED COMPONENTS DEFINITION **20**

6 SECURITY REQUIREMENTS **21**

6.1 TOE Security Functional Requirements 21

6.1.1 Security Audit(FAU) 21

6.1.2 User Data Protection (FDP) 23

6.1.3 Identification and Authentication (FIA) 24

6.1.4 Security Management (FMT) 25

6.1.5 Protection of the TSF (FPT) 26

6.1.6 TOE access (FTA) 26

6.1.7 Cryptographic operation 27

6.2 Security Functional Requirements Rationale 27

6.2.1 Coverage 27
6.2.2 Sufficiency 28
6.2.3 Security Requirements Dependency Rationale 29
6.3 Security Assurance Requirements 31
6.4 Security Assurance Requirements Rationale 32
7 TOE SUMMARY SPECIFICATION **33**
7.1 TOE Security Functionality 33
7.1.1 Authentication 33
7.1.2 Access control 33
7.1.3 Auditing 35
7.1.4 Communications security 35
8 ABBREVIATIONS, TERMINOLOGY AND REFERENCES **36**
8.1 Abbreviations 36
8.2 Terminology 36
8.3 References 36

List of Tables

Table 1: Asset List 13
Table 2: Agent List 13
Table 3: Mapping Objectives to Threats 17
Table 4: Mapping Objectives for the Environment to Threats, Assumptions 17
Table 5: Sufficiency analysis for threats 18
Table 6: Sufficiency analysis for assumptions 19
Table 7: Mapping SFRs to objectives 28
Table 8: SFR sufficiency analysis 29
Table 9: Dependencies between TOE Security Functional Requirements 31

List of Figures

Figure 1: Hardware and software environment 6
Figure 2: TOE Software architecture 7
Figure 3: TOE Logical scope 8

1 Introduction

This Security Target is for the evaluation of Huawei Integrated Management Application Platform which is the infrastructure for all the huawei's Operations Support System (OSS).

1.1 ST reference

Title: Huawei Integrated Management Application Platform Security Target
Version: V0.63
Author: Huawei
Publication date: 2011-08-24

1.2 Target of Evaluation（TOE）reference

TOE name: Huawei Integrated Management Application Platform
TOE version: Version 3 Release 1 C05 SPC500
TOE Developer: Huawei
TOE release date: 2011-07-24

Note: It is also used the acronym iMAP as TOE reference in the Security Target and ancillary documents for CC evaluation.

1.3 TOE Overview

Operation Support System (OSS) is a software application used by operators to manage network elements (NEs, which is hardware device) in telecommunication domain. Usually an OSS will make network connection to NEs, collect alarms and performance statistic data generated in these NEs, and then display these information in an user interface (usually a graphic user interface, GUI). An OSS also provides features to view and modify NE configuration.

iMAP is a software platform that help to build an OSS application. And iMAP is also an Client-Server kind of application by itself, providing the basic functionality of an OSS. It provide the system management feature for the OSS itself (like service start/stop/status monitor) and implement some common feature of the OSS, like alarm management/security management. To build a complete OSS system, the developers will need to implement new service modules like performance management/configuration management that are more specific to individual product domain. Currently in Huawei, different product domains have their own OSS applications based on iMAP, for example, M2000 for wireless domain, U2000 for core network domain, N2000 for network domain and T2000 for transmission domain.

The ST contains a description of the security objectives and the requirements, as well as the necessary functional and assurance measures provided by the TOE. The ST provides the basis for the evaluation of the TOE according to the Common Criteria (CC) for Information Technology Security Evaluations.

1.3.1 TOE usage

As a software platform, iMAP provide following component to application developer to help them build their own OSS system:

- Common utility: these are software Application Programming Interfaces(API) the developer can use in their application directly. For example, iMAP provide APIs to do string conversion between different code set, so the application developer do not need to implement this feature themselves.
- Service framework: a service framework provide common functionality for certain feature, the application developer will need to add their own specific program logic according to the application requirement to implement the feature. For example, OSS system need to communicate with network elements, different network elements have different application interfaces, but for network protocol, most of them are using TCP connection, so iMAP provide a mediation framework that handle the network communication, application developer only need to add code to prepare and parse the data package for the application interface.
- Common service: Some requirements are common to all of the OSS systems, for example, the requirement for Alarm Management Subsystem is common, iMAP implement this subsystem as a completed common service so that the OSS developer do not need to developer their own.

As the OSS infrastructure, iMAP provide extensive security features, including account based system access control that enforce only authenticated user can access authorized system features; auditing of security-relevant user activities; as well as the enforcement of network transmission against data peeking; Alarm processing is used to collect NEs alarms and then analyze these; system management to manage OSS own services.

The major security features implemented by iMAP and subject to evaluation are:

- Authentication. Operators using the GUI client to access the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords.
- Authorization. An authenticated user of the TOE can only perform the operations he is authorized to.
- Communications security. The TOE support SSL/SFTP protocol in communications between client and server side; support SNMPv3 protocol in communications between server side and northern bound.
- Auditing. Audit records are created for security-relevant events relative to the use of The TOE.
- Security function management. The TOE offers management functionality for its security functionality.
- Access Control List. From only the specified IP address or Network address can users log on to the system.
- User session monitoring. Users who are authorized to perform this operation are allowed to monitor online users and their behaviors. Those sessions that are doing anything suspicious could be invalidated immediately to prevent damages to the system and its data information from happening.

1.3.2 TOE type

The TOE is a software platform that helps to build an OSS application. And the TOE is

also an Client-Server kind of application by itself, providing the basic functionality of an OSS. It provide common utilities, service framework and common services to application developers to Simplify and accelerate the development process.

The TOE implements basic functions of OSS: security features, including account based system access control that enforces only authenticated user can access authorized system features; auditing of security-relevant user activities; as well as the enforcement of network transmission against data peeking; Alarm processing is used to collect and analyze NEs alarms; system management to manage services of the OSS its own.

1.3.3 Non TOE Hardware and Software

This section describes the Supported Platforms and hardware Environment of the TOE.

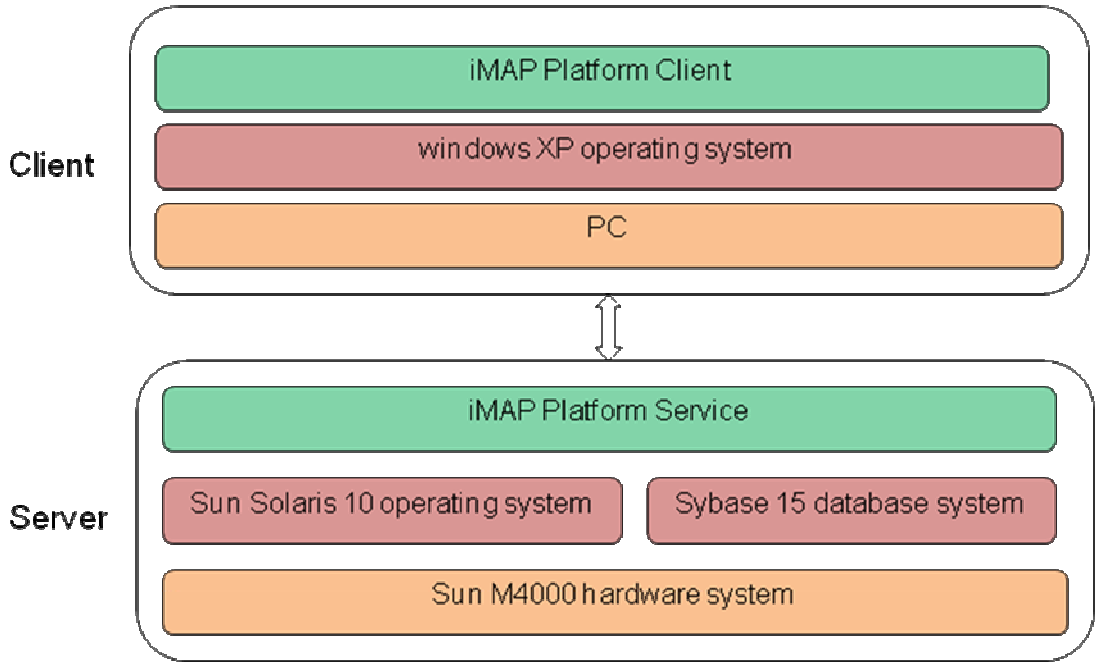

Figure 1: Hardware and software environment

The TOE requires an operating environment which contains a Sun M4000 server with Sun Solaris 10 operating system installed Sybase 15 database system which also runs on M4000 server, a PC with Windows XP operating system and physical network connection between M4000 server and the PC client.

1.4 TOE Description

1.4.1 Architectural overview

This section will introduce the TOE from a physical architectural view and a software architectural view.

1.4.1.1 Physical Architecture

The TOE need the following hardware and software requirements being satisfied: A Sun M4000 hardware system with Sun Solaris 10 operating system and Sybase 15 database system installed to be deployed on. A PC with Windows XP operating system installed is required to run the software client. Meanwhile, the physical network connection between the client and server is mandatory.

All theses hardware and software components required for operating environment are not included in this evaluation.

1.4.1.2 Software Architecture

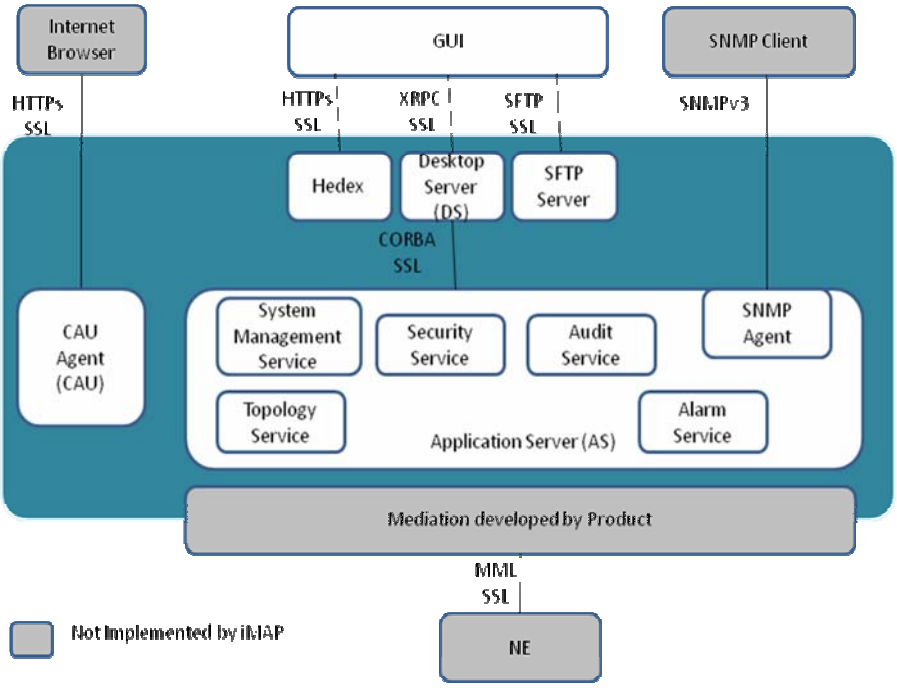

Figure 2: TOE Software architecture

The software architecture of the TOE is an enhancement of the traditional Client/Server (C/S) architecture, which consists of three layers:

- AS, Application Server
- DS, Desktop Server
- Client

Note that the **Application Server** is the main functional layer, the OSS features of data collecting, data processing and data configuration are implemented in this layer, and system authentication and authorization features are also included as well.

The **Desktop Server** layer can be considered as a data cache layer, it provides data query feature. Client layer only communicates with desktop server layer, the data retrieving requests are fulfilled in DS while the data modification requests are passed down to AS layer.

The **Client** layer is the graphic user interface (GUI) of OSS system, it provides data

presentation, and data query and data configuration interfaces to end users.

As illustrated above, almost all the system modules consist of three components which located in these three layers separately.

1.4.2 Scope of Evaluation

This section will define the scope of the Huawei's iMAP OSS Platform to be evaluated.

1.4.2.1 Physical scope

As a software application platform, the TOE is a software to be installed on specified hardware server and do not contain any hardware itself.

However, the TOE require an operating environment which contain a Sun M4000 server with Sun Solaris 10 operating system installed, sybase 15 database system which also run on M4000 server, a PC with Windows XP operating system and physical network connection between M4000 server and the PC client.

1.4.2.2 Logical scope

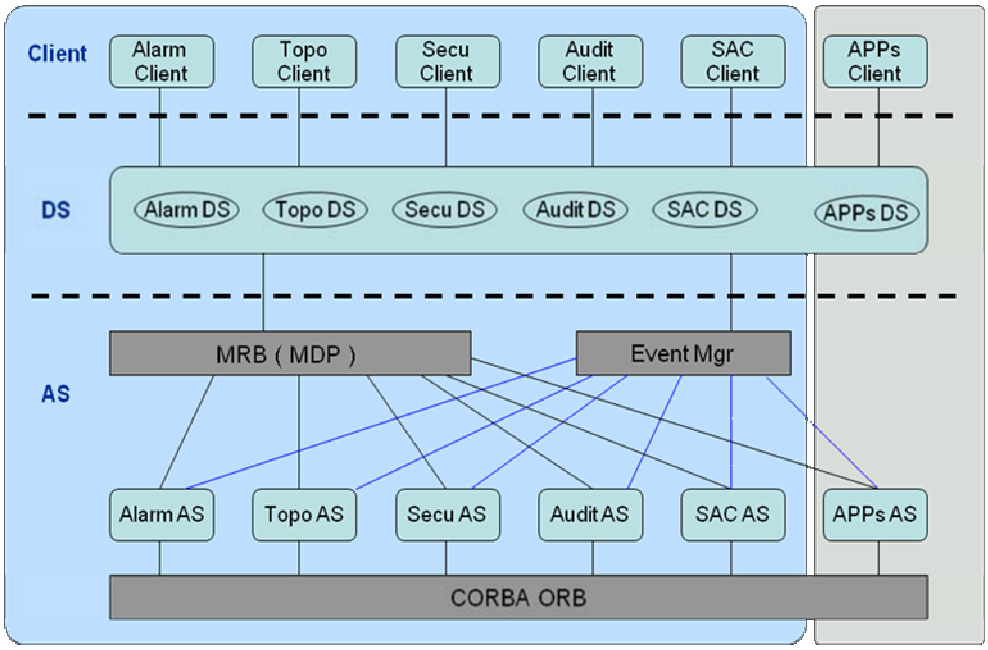

Figure 3: TOE Logical scope

As illustrated in the figure above, the logical boundary of the TOE is represented by the elements that are displayed within the large rectangle with light blue background. The OSS system which based on iMAP OSS Platform (this TOE) will develop new service module as displayed within the small rectangle with light grey background, these elements are not included in this evaluation.

The main components of the TOE described as below:

- Security Service, provide system authentication and authorization features

- Audit Service, record and display different types of audit info including security audit
- System Administration and Control Service (SAC), manage all the system services, monitor their status, and reload failed services.
- Alarm Service, receive alarm from different sources including security relevant alarm, and info user by several means(GUI display, Email, Short message to phone)
- Software bus, support both raw TCP and SSL network transmission

Based on physical scope and logical scope described so far, a list of configuration is to be added:

- Raw TCP network connection (no encryption) between different OSS components is not supported in this evaluated configuration thus raw TCP transmission mode is disabled during this evaluation.

The environment for TOE comprises the following components:

- Computer hardware with OS system to run the TOE's AS and DS software
- Personal Computer used by administrators and operators to run the TOE's client software to access the system function
- Physical networks, such as Ethernet subnets, interconnecting various networking devices.
- Firewall: all the accesses to the TOE are performed through a firewall. Only the following communications are allowed by the firewall:

    A. TCP interface(with SSL enabled): this interface is used in communication between GUI client and the server of the TOE (XRPC protocol).

    B. SFTP interface: the TOE use this interface to communicate between the GUI and the Server.

    C. SNMPv3 interface: the TOE use this interface to communicate with upper management system and act as SNMPv3 client.

    D. CAU interface for updating the software.

    E. Hedex interface for providing on-line help.

1.4.3 Summary of Security Features

1.4.3.1 Authentication

For any users of the TOE, before he can access any feature of the system from client software, the TOE always enforced a login process. The TOE will authenticate users by user name and password.

1.4.3.2 Authorization

The administrator can use the security management GUI to assign access to user accounts. When a user login to the system, the TOE will only display the network elements and information (like alarm or audit record) the user has been authorized to access, and the user can only perform authorized operation to these network element and information.

The administrator can choose to use a role-based access control policy or to assign access to individual user separately.

1.4.3.3 Auditing

The TOE generates audit records for security-relevant management actions and stores the audit records in database:

- User login / logout, a failed login attempt is also recorded.
- User account create / delete / modification
- Grant or revoke access right from user account

Attempts of management operation regardless success or failure is logged, along with user id, source IP address, timestamp etc.

A query GUI is provided for administrators to inspect the audit log, also backup feature for audit record is provided.

1.4.3.4 Security function management

A security management GUI is provided in client software which only can only be accessed by users that belong the Security Manager Group or the super user admin.

These administrators (Security Manager Group or the super user admin) use security management GUI to manage user accounts, grant access rights to users, setup system access control policy, etc.

1.4.3.5 System access control policy

The TOE offers a feature Access Control List (ACL) for controlling which terminals can be used to login to the TOE. The ACL is based on IP address, the administrators can specify individual IP address or IP address range in the ACL of a user account, the user then only can login to the TOE from terminals that use one of these IP address.

The administrators also can control the time period which a user can login to the TOE, for example, the administrator may want to limit the valid time period of a normal user account to 9:00 – 17:00 working day (Monday to Friday).

1.4.3.6 User session monitoring.

All online user sessions and their latest behaviors are monitored and presented in the real-time. Once any of these sessions seems to be suspicious, the system administrator can immediately invalidate the sessions by kicking the sessions out of the system to prevent it from damages.

1.4.3.7 Communication security

The TOE has following communication security enforcement:

- SSL enabled tcp connection to communicate between GUI client and the TOE and between different components of the TOE
- SFTP to communicate between GUI and the Server
- SNMPv3 to communicate with external upper management system

1.4.3.8 Functionality without security claims

This evaluation does not make security claims with regard to the following functionality offered by the TOE:

- No claims are made with regard to the logging function for network traffic.
- Application proxies, attack defense mechanisms, IPSec and VPN functionality can be used where available, but have not been evaluated. It will be disabled during evaluation.
- High availability (HA) features, such as the automatic switch-over to the redundant host in case of hardware failure, may be provided as part of OSS solution, but not included in this evaluation.
- Separate tools may be provided to enforce security of underlie operating system and database system, but not included in this evaluation.

2 CC Conformance Claim

This ST is *CC Part 2 conformant* [CC] and *CC Part 3 conformant* [CC]. The CC version of [CC] is 3.1R3.

This ST is EAL3-conformant+ ALC_CMC.4 + ALC_CMS.4 as defined in [CC] Part 3.

No conformance to a Protection Profile is claimed.

3 TOE Security problem definition

3.1 Threats

3.1.1 Assets

The TOE has protected following assets:

Asset	Description	Type of Data
A. Configuration Data	The confidentiality, availability and integrity of the configuration data need to be protected because the data is important to keep the system function properly, for example, set the system to maintenance mode will make all users other than administrator unable to login to the system.	Configuration Data
A.NE Connectivity Data	NE Connectivity Data include network address (like IP address and port) and user account. Loss of availability and integrity will make the system to fail manage the network element. Loss of confidentiality will let the attacker gain control to the network element.	Account Data
A.Alarm Data	Alarm indicate abnormal situation of network element that need to be handled by the operator. Loss of confidentiality, availability and integrity may cause the operator fail to solve the problem in time.	Alarm Data

Table 1: Asset List

3.1.2 Agent

The threat agent of the TOE identified as following:

Agent	Description
Network attacker	A user from the management network where the TOE reside in trying to intercept the network communication and acquire valued information asset, and potentially falsify the data transferred on the network.
Unauthenticated user	A user who is able to access client software of the TOE but without a valid user account trying to gain access to the TOE.
Authenticated user	An authenticated user trying to perform operations he is not authorized to from client software

Table 2: Agent List

3.1.3 Threats

As a result, the following threats have been identified:

Threat	Attack
T.UnauthenticatedAccess	**Attacker:** Unauthenticated user **Asset:** A. Configuration Data / A.NE Connectivity Data / A.Alarm Data **Attack:** A user without a valid user account of the TOE successfully bypass the authentication process and pretend to be an authenticated user of the TOE, then gain access to the assets. Depend on the authorization of the user he pretend to be, he may compromise the availability, integrity and confidentiality of all the assets.
T.UnauthorizedAccess	**Attacker**: Authenticated User **Asset**: A. Configuration Data / A.NE Connectivity Data / A.Alarm Data **Attack**: An authenticated user successfully bypass the authorization control of the TOE and gain access to the assets he is not authorized to. he may compromise the availability, integrity and confidentiality of all the assets.
T.Eavesdrop	**Attacker**: Network attacker **Asset**: A.NE Connectivity Data/ A. Configuration Data / A.Alarm Data **Attack**: A network attacker from management network successfully intercept the data communication of the TOE and compromise the confidentiality of NE Connectivity, alarm and configuration Data and the integrity of NE Connectivity and alarm Data.
T. BehaviorDeny	**Attacker**: Authenticated User **Asset**: A. Configuration Data / A.NE Connectivity Data / A.Alarm Data **Attack**: An authenticated user perform an authorized operation by means or by mistake, compromise the availability and integrity of the assets(for example, delete NE connectivity data), and deny what he has done.

3.2 Assumptions

3.2.1 Environment of use of the TOE

3.2.1.1 Physical

A.PhysicalProtection It is assumed that the hardware system (usually a unix server) which the components of the TOE reside in is protected against unauthorized physical access.

3.2.1.2 NetworkSegregation

A.NetworkSegregation	It is assumed that the sub-network which the TOE reside in is separate from the application (or, public) networks. The communications with the TOE are performed through a firewall. See section 1.4.2.2 Logical scope for more information.

3.2.1.3 Operating System

A.OperatingSystem	it is assumed that the operating system for the TOE has been hardened properly and patched in time, so there is no security weakness, and thus protected against unauthorized access.

3.2.1.4 DataBase

A.DataBase	It is assumed that the database system used by TOE has been hardened properly and patched in time, so there is no security weakness, and thus protected against unauthorized access.

3.2.1.5 Administrator

A.Administrator	It is assumed that the superuser admin and the users that belong to the SMManagers and Administrator groups behave correctly and do not perform harmful operation in the TOE. Also, the users of the underlying operating system.

4 Security Objectives

4.1 Objectives for the TOE

The following objectives must be met by the TOE:

- **O.Communication** The TOE must implement logical protection measures for network communication between different components of the TOE and in the communication between the server and SNMP client.
- **O.Authorization** The TOE shall implement authorization measures to restrict the functionality that is available to individual user account.
- **O.Authentication** The TOE must authenticate user before he can access any functionality of the TOE. The TOE shall provide configurable system policy to restrict user session establishment.
- **O.Audit** The TOE shall provide functionality to generate audit records for security-relevant user actions and provide functionality for authorized user to review these audit records.

4.2 Objectives for the Operational Environment

- **OE.Physical** The hardware system which the TOE server is running on shall be protected against unauthorized physical access.
- **OE.NetworkSegregation** The operational environment shall provide protection to the network in which the TOE hosts by separating it from the application (or public) network. A firewall shall be installed in the environment.
- **OE.OperatingSystem** The operating system which the TOE server is running on shall be protected against unauthorized access.
- **OE.DataBase** The database system used by the TOE shall be protected against unauthorized access.
- **OE.Administrator** The superuser admin and the users that belong to the SMManagers and Administrator groups of the TOE should behave correctly and should not perform harmful operation in the TOE. Also, the users of the underlying operating system.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective is at least covered by one threat or policy.

Objective	Threat
O.Communication	T.UnauthorizedAccess T.UnauthenticatedAccess T.Eavesdrop

O.Authentication	T.UnauthenticatedAccess T.UnauthorizedAccess
O.Authorization	T.UnauthorizedAccess
O.Audit	T.UnauthenticatedAccess T.UnauthorizedAccess T.BehaviorDeny

Table 3: Mapping Objectives to Threats

The following table provides a mapping of the objectives for the operational environment to assumptions, threats and policies, showing that each objective is at least covered by one assumption, threat or policy.

Environmental Objective	Threat / Assumption
OE.Physical	A.PhysicalProtection T.UnauthenticatedAccess T.UnauthorizedAccess
OE.NetworkSegregation	A.NetworkSegregation
OE.OperatingSystem	A.OperatingSystem T.UnauthenticatedAccess T.UnauthorizedAccess
OE.DataBase	A.DataBase T.UnauthenticatedAccess T.UnauthorizedAccess
OE.Administrator	A.Administrator T.BehaviorDeny

Table 4: Mapping Objectives for the Environment to Threats, Assumptions

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T.UnauthenticatedAccess	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication). The implementation of a network communication protection is able to help by avoiding attackers eavesdrop account information from network.(O. Communication) The audit feature will help to find out the illegal login

	attempt to the TOE and take countermeasure in time. (O.Audit) The protection of hardware environment and operating system and database will help to avoid the attackers gain access to the account information. (OE.Physical, OE.OperatingSystem, OE.DataBase)
T.UnauthorizedAccess	The threat of unauthorized access is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication) and an access control mechanism (O.Authorization). The implementation of a network communication protection is able to help by avoiding attackers eavesdrop account information from network (O. Communication) and thus gain unauthorized access to the TOE. The audit feature will help to detect the operation user account involved in the unauthorized access, and take countermeasure in time. (O.Audit) The protection of hardware environment and operating system and database will help to avoid the attackers gain access to the account information and and thus gain unauthorized access to the TOE. (OE.Physical, OE.OperatingSystem, OE.DataBase)
T.Eavesdrop	The threat of eavesdropping is countered by requiring communications security via SSL network communication between different components of the TOE and in the communication between the server and SNMP client (O. Communication).
T. BehaviorDeny	The threat of behavior deny is countered by record all the security-relevant operation and put the record in database, provide review feature for audit record. (O.Audit) The superuser admin and the users that belong to the SMManagers and Administrator groups of the TOE should behave correctly and shall not perform harmful operation in the TOE. Also, the users of the underlying operating system. (OE.Administrator)

Table 5: Sufficiency analysis for threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Assumption	Rationale for security objectives
A.PhysicalProtection	The assumption that the TOE will be protected against unauthorized physical access is expressed by a corresponding requirement in OE.Physical.

A.NetworkSegregation	The assumption that the TOE is not accessible via the application networks hosted by the networking device is addressed by requiring just this in OE.NetworkSegregation and installing a firewall.
A.OperatingSystem	The assumption that the TOE will be protected against unauthorized access is expressed by a corresponding requirement in OE.OperatingSystem
A. DataBase	The assumption that the database used by the TOE will be protected against unauthorized access is expressed by a corresponding requirement in OE.DataBase.
A. Administrator	The assumption that superuser admin and the users that belong to the SMManagers and Administrator groups of the TOE should behave correctly and shall not perform harmful operation in the TOE. Also, the users of the underlying operating system is expressed by a corresponding requirement in OE. Administrator.

Table 6: Sufficiency analysis for assumptions

5 Extended Components Definition

No extended components have been defined for this ST.

6 Security Requirements

6.1 TOE Security Functional Requirements

6.1.1 Security Audit(FAU)

6.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **[selection: <u>detailed</u>]** level of audit; and

c) **[assignment:** ***user login, logout***

d) ***user account management***

1. ***user account create, delete, modify***

2. ***change user password***

3. ***grant access right to user account***

e) ***user group(role) management***

1. user group create, delete, modify

2. grant access right to user group

f) ***security policy management***

1. modify password policy

2. modify user account policy

g) ***user session management***

1．Kick out individual user session

h) ***ACL management***

1．ACL create, delete, modify

2．Specify ACL for individual user account **]**

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 **(Based on audit event type, the following information may not be applicable)**:

i. **[assignment:** ***Operation Name***

ii. ***Risk Level***
iii. ***User***
iv. ***Operation Terminal***
v. ***Operation Object***
vi. ***Additional detail Information*** **]**

6.1.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **[assignment: *authorized users*]** with the capability to read **[assignment: *all information*]**from the audit records.
FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **[assignment: *selection*]** of audit data based on **[assignment: *operation user/operation terminal/operation result/risk level/operation duration/operation name/certain characters contained in detailed information field.*]**

6.1.1.6 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall **[assignment: *export oldest data to file(s)*]** if the audit trail exceeds **[assignment: *30 days of log storage*.]**

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_ACC. 2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the **[assignment: *iMAP access control policy*]** on **[assignment:*users as subjects, managed objects as objects*]** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.1.2.2 FDP_ACF.1 Security attributes based access control

FDP_ACF.1.1 The TSF shall enforce **[assignment: *the iMAP access control policy*]** to objects based on the following:

a) [**assignment: *users and their following security attributes:***

i. the group(s) to which the user bind

b) Managed Objects and their following security attributes:

i. operation(s) that can be performed on managed object **]**

Please refer to 6.1.2.1 for definition of managed object.

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) **[assignment: *the user has been granted authorization for the Managed Object targeted by the request, and***

b) ***the user is associated with operation(s) of the Managed Object targeted that contains the requested operation(s)*** **]**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

a) [assignment: *None*]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:.

a) [assignment:*None*]

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **[selection: an administrator configurable positive integer within [assignment: *1-99*]]**unsuccessful authentication attempts occur related to **[assignment: *user login from client GUI*]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **[selection:met]**, the TSF shall **[assignment: *lock the user account and generate an alarm event.*] .**

NOTE: The administrators can check the alarm in alarm GUI.

6.1.3.2 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) **[assignment: *Account status;***

b) Account password;

c) Password status;

d) Password validity days;

e) Maximum number of online users;

f) Wait time for auto exit;

g) Inactive user policy;

h) Login duration control;

i) User groups;

j) User domain;

k) Operation rights;

l) ACL. **]**

6.1.3.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet:

a) **[assignment: *Secret length should be within 6-16 characters***

b) Secret should contain at least one letter and one number

c) ***When an individual user changes his secret, the secret should be different from the last 5 secrets he has used.*** **]**

6.1.3.4 FIA_UAU.2 User authentication before any action

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.

6.1.3.5 FIA_UID.2 User identification before any action

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.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce **[assignment: *the iMAP access control policy*]** to restrict the ability to **[selection: query, modify]** the security attributes **[assignment: *identified in FDP_ACF.1*]** to **[assignment: *Admin user and users who belong to the Security Manager group*]**

6.1.4.2 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **[assignment: *iMAP access control policy*]** to provide **[selection: permissive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow **[assignment: *Admin user and users who belong to the Security Manager group*]** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 FMT_MSA.4 Security attribute value inheritance

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes:

a) [assignment: *The user's rights that he inherits from the groups that he belongs to*;]

6.1.4.4 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

a) **[assignment:** ***grant operation right to user***
b) ***user management, user group management***
c) ***definition of Managed Objects as object set***
d) ***definition of Operations as operation set***
e) ***definition of IP addresses and address ranges that will be accepted as source addresses in client session establishment requests***
f) ***definition of user account locking policy***
g) ***account status specify if user allow to login***
h) ***monitor user session and user operation***
i) ***Modify the policy of user password***
j) ***the time period when user allowed to login***
k) ***Audit Date export Configuration*****]**

6.1.4.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **[assignment:** ***the super user admin, Administrators group, security manager user group, Monitors group, Operators group, Normal group and administrator-defined roles.*** **]**
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from **[selection: disclosure]** when it is transmitted between separate parts of the TOE.

6.1.6 TOE access (FTA)

6.1.6.1 FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

6.1.6.2 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on

a) **[assignment: *date and time***

b) ***account locking status***

c) ***source IP address.*** **]**

6.1.7 Cryptographic operation

6.1.7.1 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[assignment: *cipher and decipher operations*]** in accordance with a specified cryptographic **algorithm [assignment: *DES*]** and cryptographic key sizes **[assignment: *56 bits*]** that meet the following: **[assignment: *None*]**.

Application Note: DES algorithm is used to cipher/decipher the communication between the server and a SNMP client.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

	O.Audit	O.Authentication	O.Authorization	O. Communication
FAU_GEN.1	×			
FAU_GEN.2	×			
FAU_SAR.1	×			
FAU_SAR.2	×			
FAU_SAR.3	×			
FAU_STG.3	×			
FDP_ACC.2			×	
FDP_ACF.1			×	

FIA_AFL.1		×		
FIA_ATD.1		×	×	
FIA_SOS.1		×		
FIA_UAU.2		×	×	
FIA_UID.2	×	×	×	
FMT_MSA.1			×	
FMT_MSA.3			×	
FMT_MSA.4			×	
FMT_SMF.1	×	×	×	
FMT_SMR.1			×	
FPT_ITT.1				×
FTA_TAB.1		×		
FTA_TSE.1		×		
FCS_COP.1				×

Table 7: Mapping SFRs to objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Security objectives	Rationale
O.Audit	The generation of audit records is implemented by **FAU_GEN.1**. Audit records are supposed to include user identities (**FAU_GEN.2**) where applicable, which are supplied by the authentication mechanism (**FIA_UID.2**). Audit records are in a string format, regular expressions are provisioned to read and search these records (**FAU_SAR.1, FAU_SAR.3**),and only authorized user can read audit records(**FAU_SAR.2**). Functionality to delete the oldest audit file is provided if the size of the log files becomes larger than the capacity of the store device (**FAU_STG.3**). Management functionality for the audit mechanism is spelled out in (**FMT_SMF.1**).

O.Communication	Communications security is implemented by the establishment of a secure communications channel: between separate parts of TOE is protected by **FPT_ITT.1, the data communication between the TOE and other IT product(SNMP) is protected by ciphering the communication (FCS_COP.1)**
O.Authentication	User authentication is implemented by **FIA_UAU.2** and supported by individual user identifies in **FIA_UID.2**. The necessary user attributes (passwords) are spelled out in **FIA_ATD.1**. The authentication mechanism supports authentication failure handling (**FIA_AFL.1**), restrictions as to the validity of accounts for logon (**FTA_TSE.1**), and a password policy (**FIA_SOS.1**). Warning of Non-Authorization access is provided in **FTA_TAB.1**. Management functionality is provided in **FMT_SMF.1**.
O.Authorization	User need to be authenticated first before being allowed to perform any operations in the TOE(**FIA_UAU.2**). The requirement for access control is spelled out in **FDP_ACC.2**, and the access control policies are modeled in **FDP_ACF.1**. Unique user IDs are necessary for access control provisioning (**FIA_UID.2**), and user-related attributes are spelled out in **FIA_ATD.1**. Access control is based on the definition of roles as subject and functions as object(**FMT_SMR.1**).Management functionality for the definition of access control policies is provided (**FMT_MSA.1**, **FMT_MSA.3**, **FMT_MSA.4, FMT_SMF.1**).

Table 8: SFR sufficiency analysis

6.2.3 Security Requirements Dependency Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

The following table demonstrates the dependencies of SFRs modeled in CC Part 2

and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	Not resolved. The audit time is depended on the reliable time stamp. Reliable time stamp is depended on external time sources, such as GPS clock.
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.3	FAU_STG.1	Not resolved. The audit records are stored in a database outside the TOE. The protection of audit trail storage depended on the external database system.
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	
FIA_SOS.1	None	
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	None	
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2
FMT_SMF.1	None	

FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_ITT.1	None	
FTA_TAB.1	None	
FTA_TSE.1	None	
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	Not resolved. The key used to cipher the communication is configured in the TOE during the installation process. Therefore, no mechanism is provided in the TOE neither to import the key nor to generate it. The key is never zeroized given that it is necessary for the operative of the TOE.

Table 9: Dependencies between TOE Security Functional Requirements

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components as specified in [CC] Part 3+ ALC_CMC.4 + ALC_CMS.4. No operations are applied to the assurance components.

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level
Development	ADV_ARC	1
	ADV_FSP	3
	ADV_IMP	NA
	ADV_INT	NA
	ADV_SPM	NA
	ADV_TDS	2
Guidance documents	AGD_OPE	1
	AGD_PRE	1
Life-cycle support	ALC_CMC	4
	ALC_CMS	4
	ALC_DEL	1
	ALC_DVS	1
	ALC_FLR	NA
	ALC_LCD	1
	ALC_TAT	NA
Security Target evaluation	ASE_CCL	1
	ASE_ECD	1

	ASE_INT	1
	ASE_OBJ	2
	ASE_REQ	2
	ASE_SPD	1
	ASE_TSS	1
Tests	ATE_COV	2
	ATE_DPT	1
	ATE_FUN	1
	ATE_IND	2
Vulnerability assessment	AVA_VAN	2

6.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

7 TOE Summary Specification

7.1 TOE Security Functionality

7.1.1 Authentication

The TOE offers the enforcement of timer-based account lockouts: administrators can specify after how many consecutive failed authentication attempts an account will be temporarily locked, and whether the counter for failed attempts will be reset automatically after a certain amount of minutes. (**FIA_AFL.1**)

Authorized administrators are able to configure a system-wide password policy that is then enforced by the TOE. Besides the minimum length of the password, which can be set to be between 6 and 16 characters, administrators have the option to enforce the use of specific characters (numeric, alphanumeric low or capital, and special characters). (**FIA_SOS.1**)

The TOE authenticates the users in the management network based on individual user IDs and passwords. User IDs are unique within the TOE and stored together with associated passwords and other security attributes in the TOE's configuration database. (**FIA_ ATD.1**)

The TOE can identify administrators in the management network by a unique ID and enforces their authentication before granting them access to the TSF management interfaces. Warning of "error username or password" will be prompted when the user fails to provide a correct username or password. (**FIA_UID.2**)

Authentication based on user name and password is enforced prior to any other interaction with the TOE for all external interfaces of the TOE (**FIA_UAU.2**)

Before establishing a user session, the GUI will display an advisory warning message regarding unauthorized use of the TOE. (**FTA_TAB.1**)

If applicable, i.e., if an administrator has specified values for these parameters for a specific user, the TOE will deny authentication of the user if the user tries to authenticate in a timeframe that lies outside of the "login start time" and "login end time" specified for the user. When the user use an expired password to login, the system will refuse the login request, the user must request the administrator to reset his password (the Administrator can deactivate the password expiration policy).

The administrator can monitor online user sessions in GUI, he can see the operations executed in each user session. If an user session behave improperly, the administrator can force the user to logout.

(**FMT_SMF.1**)

The TOE provide login time control mechanism: Each account can be configured with the login time segment, including the valid date range, time segment, and week restriction. Any login is prohibited beyond the configured time segment. If the IP address of the client is not in the specified IP address range from which the user is allowed to login, the login request will be refused. Also a locked user account can not be used to login to the TOE. (**FTA_TSE.1**)

7.1.2 Access control

The TOE controls which operations users can perform on Managed Objects. Managed Objects(MO) are logical representations of product units that can be managed using the TOE. For example, the TOE itself is a MO. The individual network elements that

are managed by the TOE are Managed Objects.

Access control is enforced two-fold:

1. Managed Object authorization: operators can be authorized to see a Managed Object (for example, in the topology GUI)
2. Operation authorization: operators can be authorized to perform specific operations on a Managed Object (for example, to modify configuration data of a network element)

(**FDP_ACC.2**)

In order to implement role-based access control, users can be grouped into User Groups. Users and User Groups can be given MO authorization (also referred to as “Application rights” or “Network element rights”) for specific Managed Object. This merely represents the fact that users are authorized to know about the existence of the MO (the MO will show up in GUI, etc.) – additional authorization to perform any specific management commands on the MO are then assigned in separate steps.(**FDP_ACF.1**)

The authorization specifies the operations a user can perform on a specific MO, such as “Application rights: Create Subnet” to create a subnet on topology GUI.

The TOE provide device set and operation set to help authorized administrators to do authorization. A device set contain a list of MOs and a operation set contain a list of operation that can be performed on these MOs. Users or User Groups can be assigned to a device set with a corresponding operation set, which grants them the right to perform the operations specified in the operation set on the MOs specified in the device set. The administrators can define device set and operation set to reflect authorization needs. (**FMT_MSA.1, FMT_SMF.1**)

As a result, authorized administrators who add new users to the system must specify which MOs these users are allowed to see (MO authorization) and which operations the users is allowed to perform on these MOs. (**FMT_MSA.3**)

There are some predefined special roles exist in the TOE:

1. The super user admin has all the rights in the system.
2. A Security Manager group, only the users belong to this group will be granted the right to access security management GUI and perform security management related job. The rights assigned to Security Manager group are all security management related and there is no way to assign these rights to other roles in the TOE, so it is impossible to create a new role with similar rights of Security Manager group.
3. An Administrators group, users belong to this group can manage all the MOs in the TOE, except for security management.
4. Three common groups (Monitors group, Operators group, Normal group) are created automatically for convenience, there are no access rights assigned to these groups by default.

In order to implement role-based access control, users can be grouped into User Groups. The following pre-defined roles are included in the TOE: the super user admin, administrator group, security manager group and three common groups (Monitors group, Operators group, Normal group). (**FMT_SMR.1, FMT_MSA.4**)

7.1.3 Auditing

The TOE generates audit records for security-relevant events. (Please refer to FAU_GEN.1 for a list of event types, and the type of information recorded.)

The auditing functionality of the TOE cannot be started or stopped independently from the operational TOE. (**FAU_GEN.1**)

Where appropriate, the data recorded with each audit record includes the unique user ID associated with a subject during authentication. (**FAU_GEN.2**)

If the audit records stored in any of the logs exceed specified days, the TOE will extract the expired records from the database and transfer them into a flat file in the operational environment in order to keep the database from overflowing.

If the files in the operational environment use more space than a defined limit, they will be deleted. (**FAU_STG.3**)

Only authorized users can use GUI to review the audit records available in the database. The GUI offers search functionality based on time intervals, user IDs, interface, workstation IP, result, and operation name. (**FAU_SAR.1, FAU_SAR.2, FAU_SAR.3**)

7.1.4 Communications security

The TOE provides communications security for network connections to the TOE . This includes connections via the following interfaces:

1. GUI connections between clients and the server (using SSL) (**FTP_ITT.1**)

   SFTP connections between the server and the GUI(using SSL) (**FTP_ITT.1**)
2. SNMP connections between the server and external SNMP clients (using SNMPv3) (**FCS_COP.1**)

8 Abbreviations, Terminology and References

8.1 Abbreviations

CC	Common Criteria
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
PP	Protection Profile
SFR	Security Functional Requirement
NE	Network Element
GUI	Graphical User Interface
iMAP	Integrated Management Application Platform
MO	Managed Object

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrator: An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE's point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.

Operator See User.

User: A user is a human or a product/application using the TOE.

8.3 References

[CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. July 2009. Version 3.1 Revision 3.

[CEM] Common Methodology for Information Technology Security Evaluation. July 2009. Version 3.1 Revision 3.