LABRİS

LABRİS v2.2.1 COMMON CRITERIA EAL 4+ (ALC_FLR.2)
EVALUATION PROJECT

LABRIS v2.2.1

SECURITY TARGET

Revision No	36		
Revision Date	20.10.2016		
Document Code	LABRIS-CC-ST		
File Name	LABRIS_ST_V36.DOC	**Language**	ENGLISH
Project	LABRİS v2.2.1 COMMON CRITERIA EAL 4+ (ALC_FLR.2) EVALUATION PROJECT		
Title	LABRIS v2.2.1 SECURITY TARGET		
Category	DELIVERABLE		

Prepared By	Oğuz Yılmaz

Revision History

Revision No	Revision Reason	Revision Date
01	First Release	10.9.2006
02	ST reviewed and formatted	10.11.2006
03	ST reviewed and formatted	10.12.2006
04	TOE Summary Specification, rationale and requirements added.	20.03.2007
05	Functions are added	18.04.2007
06	Operations are applied	21.04.2007
09	Missing parts are completed, document re-formatted	10.08.2007
10	Document Revised	13.08.2007
11	Document revised according to first review report	11.09.2007
12	Document is revised according to second review report	12.09.2007
13	Document name changed Developer field from Approval entry removed Date fields in the document has changed FAU_STG.1.1 Strikethrough on ”unauthorized” word removed FAU_SAR.3 “c)range of IP addresses” deleted FDP_IFF.1.1 “• [and schedule, defined by days of the week and start/stop time]].” Part removed FMT_MOF.1.1 “Permission to” part is erased from “c)”, “d)”,”e)”,”f)”,”g)” “create” and “empty” is erased from “e” FMT_MSA.1.1 “query” word is erased FMT_SMF.1.1 “empty” word is erased form “e)” F.MMI “create” and “empty” is deleted and “delete” is added to “e)” F.AUDPROT has changed F.FWPOLICY “vi) schedule, defined by days of the week and start/stop time.” Entry removed F.ADMIN has changed	04.02.2008
14	Document is revised according to fourth review report Baran Erdoğan removed from project staff Section 5.3 Security Requirements for the IT Environment moved as 5.1.3 TOE name is changed ST overview and TOE description updated Explanations of changes in FAU_STG.1.2, FAU_STG.4.1 and FIA_UAU.1.1 added to Rationale for Security Functional Refinements TOE boundary figure changed. Strength of Function Claim and Strength of function Rationale sections updated. Security Objectives for TOE and IT Environment section added	12.03.2008
15	Topology figure added to Physical Description section. Security Target Overview and TOE Description section is improved	08.04.2008
16	Topology figure is updated. Table 9 Mapping of Objectives to Threats and Assumptions is added. Threats partially met by the TOE and TOE Security Environment is added. Measure identifiers are updated	25.04.2008

17	Updated TOE topology figure TOE security objectives updated Rationale section updated	02.05.2008
18	TOE and Environmental thread addressing changed Environmental components changed TOE logical description updated	06.05.2008
19	Updated TOE topology figure TOE logical description updated LMCCP description added to logical description section Rationale Section for Environmental Security Objectives updated	08.05.2008
20	Security Requirements for the IT Environment refinements updated FAU_GEN SFR descriptions and tables for TOE and TOE Enviroment are updated. Rationale for TOE Security Environment Functional Requirements are updated TOE logical description figure updated	21.05.2008
21	Detailed TOE Enviromental Components List Added. Minor corrections FAU_GEN SFR descriptions.	11.07.2008
22	TOE Scope and Boundaries updated. Major changes in Security Functional Requirements TOE and IT Enviroment are handled in seperate tables in Rationale Satisfying Functional Requirements Dependencies.	15.08.2008
23	Major reduction in TOE coverage. T.MEDIAT, T.ASPOOF and T.OLDINF Removed form TOE threads. All dependent changes applied. Table 4 and 5 applied.	10.09.2008
24	FMT_MOF.1 Iteration 1 added M.DELD removed FDP_ACC.1, FDP_ACF.1 and FMT_MSA.3 added.	05.10.2008
25	TOE version changed. ACF.1.2 and ACF 1.3 added Section 7.3 updated	13.10.2008
26	Typo fixed	16.10.2008
27	Minor corrections	22.10.2008
28	Overall update, TOE version updated to 1.6.6.b, Document code fixed	02.02.2009
29	Minor corretions	12.02.2009
30	TOE version changed, minor fixes	02.03.2009
31	Updated TOE despcription, Table 4 references changed to Table 3 in Table 9	09.03.2009
32	TOE Overview updated, minor fixes	18.03.2009
33	Multiple language fixes	21.05.2009
34	Revised according to Common Criteria V3.1 R4	30.10.2013
35	Updated according to the requests on GR1	18.11.2013
36	Updated according to the requests on CC Lab	20.10.2016

Approvals

Name	Role
Oğuz Yılmaz	Technical Manager, Configuration Manager

CONTENT

1 ST INTRODUCTION 7

1.1 Security Target Identification 7

1.2 Security Target Overview 7

1.3 Operations 7

1.4 TOE Overview 7

1.4.1 Labris Management Console (LMC) Software 8

1.4.2 Labris Management Console Server (LMCS) Software 8

1.4.3 Security Features of the TOE 8

1.4.3.1 Information Flow 8

1.4.3.2 Access Control 8

1.4.3.3 Logging 8

1.5 Non TOE Hardware/Software/Firmware 8

1.6 TOE Description 9

1.6.1 Physical Scope 9

1.6.2 Logical Scope 11

2 CONFORMANCE CLAIM 12

2.1 CC Conformance Claim 12

2.2 PP and Package Claim 12

2.2.1 Protection Profile (PP) Claim 12

2.2.2 Package Claim 12

2.3 Conformance Rationale 12

3 SECURITY PROBLEM DEFINITION 13

3.1 Assumptions 13

3.2 Threats 13

3.3 Organizational Security Policies 13

4 SECURITY OBJECTIVES 15

4.1 Security Objectives for the TOE 15

4.2 Security Objectives for the Environment 15

4.2.1 IT Security Objectives for the Environment 15

4.2.2 Non-IT Security Objectives for the Environment 16

4.2.3 Security Objectives Rationale for TOE 16

4.2.4 Security Objectives Rationale for Operational Environment 18

5 EXTENDED COMPONENT DEFINITION 20

5.1.1 Reliable Time Stamps 20

6 IT SECURITY REQUIREMENTS 21

6.1 TOE Security Functional Requirements 21

6.1.1 Overview 21

6.1.2 Security Functional Requirements 22

6.1.2.1 FAU_GEN.1 Audit data generation [1] 22

6.1.2.2 FAU_SAR.1 Audit review ... 23
6.1.2.3 FAU_SAR.3 Selectable audit review ... 23
6.1.2.4 FAU_STG.1 Protected audit trail storage ... 23
6.1.2.5 FAU_STG.4 Prevention of audit data loss ... 23
6.1.2.6 FDP_ACC.1 Subset access control ... 24
6.1.2.7 FDP_ACF.1 Security Attribute Based Access Control ... 25
6.1.2.8 FIA_ATD.1 User attribute definition ... 26
6.1.2.9 FIA_UAU.1 Timing of authentication ... 26
6.1.2.10 FIA_UID.2 User identification before any action ... 26
6.1.2.11 FMT_MOF.1 Management of security functions behavior ... 26
6.1.2.12 FMT_MOF.1 (1) Management of security functions behavior ... 26
6.1.2.13 FMT_MSA.1 Management of security attributes ... 27
6.1.2.14 FMT_MSA.3 Static attribute initialization ... 27
6.1.2.15 FMT_SMF.1 Specification of Management Functions ... 27
6.1.2.16 FMT_SMR.1 Security roles ... 27
6.1.3 Security Functional Requirements Rationale ... 27
6.1.4 Rationale for Dependencies ... 30
6.2 TOE Security Assurance Requirements ... 31
6.2.1 List of Assurance Requirements ... 31
6.2.2 Security Assurance Requirements Rationale ... 32
7 TOE Summary Specification ... 33
7.1 TOE Security Functions ... 33
7.2 TOE Security Functions Rationale ... 35
8 APPENDIX ... 37
8.1 Abbreviations & Glossary ... 37

INDEX OF TABLES

Table 1 Non-TOE hardware/software/firmware 9
Table 2 Mapping of TOE Objectives to Threats 17
Table 3 Mapping of Environment Objectives to Threats, Assumptions and Policies 18
Table 4 TOE Security Functional Requirements 21
Table 5 Auditable Events by TOE 22
Table 6 Subjects and objects controlled and relevant security attributes 25
Table 7 Rationale for TOE Security Functional Requirements 28
Table 8 TOE Functional Requirement Dependencies Rationale 30
Table 9 TOE Security Assurance Requirements 31
Table 10 TOE Security Functions 34
Table 11 TOE Security Functions Rationale 35
Table 12 Abbreviations and glossary 37

1 ST INTRODUCTION

1.1 Security Target Identification

This document is the Security Target for Labris v2.2.1 and prepared in accordance to following descriptions

ST Title: Labris Version 2.2.1 Security Target, 20 October 2016, Revision 36

TOE: Labris version 2.2.1

1.2 Security Target Overview

This Security Target describes; the TOE, intended IT environment, security objectives, security requirements, security functions and all necessary rationale.

TOE targets environments, where sensitive information is processed. TOE is used in governmental institutions, commercial institutions or military institutions for secure administration of information flow between two networks, which is called as internal and external. Internal Network can access the sensitive information and is isolated from External Networks by a physical network gateway (a computer that enables the information flow between networks). TOE manages the information flow control policy of this gateway.

TOE is used in IP networks for managing security policies. It is presented as software only package or bundled with hardware with wide range scalability, ranging from Small Office Home Office (SOHO) to big enterprise networks.

TOE is designed to prevent all of the well-known attacks by providing proper predefined policies. It also enables easy configuration of wide range of security policies for information flowing through gateway.

TOE has an easy to use graphical user interface (GUI) for managing all its functionalities easily and simply, which is very important for usability and security purposes. The GUI is called LMC (Labris Management Console) and is used for managing other Labris products such as web filter, antivirus, antispam, intrusion prevention.

1.3 Operations

There are four types of operations that can be applied on functional requirements. These are;

Selection: Shown by cornered brackets and italicized text. Example: [*selection*]

Assignment: Shown by cornered brackets and regular text. Example: [assignment]

Refinement: Indicated by underlined text for additions or strikethrough text for deleted items. Example: addition ~~deletion~~

Iteration: Indicated by assigning a number at the functional component level. Example: FMT_MOF.1(1)

Marking of these operations are mandated by CC.

1.4 TOE Overview

TOE is a firewall management software collection that provides mechanisms for management and monitoring of packet filtering, IP routing, network address translation, port address translation and audit records generation. TOE is composed of two parts, which are LABRİS Management Console (LMC) Software and LABRİS Management Console Server (LMCS) software.

Labris Management Console Software is used by TOE administrators to first authenticate them to TOE and then administer it in same secure environment. They can change access rules, packet-filtering policies, routing configuration and network interface configuration. At the same time, they can review audit logs of TOE from the Labris Management Console Software. LMCCP is the network protocol between LMC Software and LMCS Software and is implemented in both TOE parts. It is an xml-based protocol. It is used with SSL sockets, which are provided by client and server operating systems. LMCCP provides reliable and secure remote connection.

1.4.1 Labris Management Console (LMC) Software

Labris Management Console Software is a client application for controlling the Labris Management Console Server Software via LMCCP (Labris Management Console Connection Protocol) protocol. LMC Software is where all user interaction occurs in TOE. It provides an easy to use graphical user interface for managing all functionalities of TOE. It is connected to LMCS Software over direct cable connection.

1.4.2 Labris Management Console Server (LMCS) Software

Labris Management Console Server Software is the server part of TOE. It provides management capabilities and audit records generation for packet filtering policies, IP routing, network and port address translation in IP networks.

1.4.3 Security Features of the TOE

1.4.3.1 Information Flow

All policies, which control the information flow between internal network and external network, are managed. These policies are related with ip packet filtering, ip routing, network address translation and port address translation.

Nodes in the external and internal network may be subject to firewall rules that are specific to their IP addresses. TOE administrator specifies these rules.

1.4.3.2 Access Control

Access control feature enables authorized administrators to manage firewall rules applied to information flow and control traffic between different network domains that are configured by TOE.

1.4.3.3 Logging

System logs are generated and saved on hard disk. All logs can be backed up by TOE. Generated audit trail is protected and new log space is opened only when the logs are backed up..

Log types are:

- System management logs.
- Information flow logs
- Operational logs

1.5 Non TOE Hardware/Software/Firmware

TOE	Labris v2.2.1 software (LMC Software, LMCS Software)
Environmental Components(LMCS)	Labris L7 Hardware: CPU : Intel Core 2 Duo E4300 RAM: 1 GB HDD: 80 GB 4 Ethernet Interfaces

	Labris Operating System v2.2.1 based on the Linux distribution CENTOS 5. Individual software components are listed below with revision numbers: iproute-2.6.18-4.el5(IP Routing) iptables-1.3.5-1.2.1 (Packet filtering, port address translation) iputils-20020927-43.el5 (IP routing) kernel-lum-2.6.18-LSG.CC.4 (Labris Operating System kernel, modified by Labris Teknoloji) sysklogd-1.4.1-39.2.lbr.10 (Audit Record Generation, modified by Labris Teknoloji) SSLv3 1024 bit
Environmental Components(LMCS)	Standard PC hardware (x86 compliant) Windows or Linux Java Virtual Machine 1.4

Table 1 Non-TOE hardware/software/firmware

1.6 TOE Description

1.6.1 Physical Scope

TOE is used for monitoring and managing the network traffic policies between two different networks.

TOE functions by configuring the information flow policy, network address translation and routing mechanisms of the security gateway of the network. According to policy specified by TOE, the security gateway denies or accepts the transmitted data to guard internal network. Internal network carries the data to be protected from the external network. External network may have malicious users or software as its users.

Topology example in Figure 1 shows the physical structure of the TOE. Two internal networks are represented with DMZ and NET2. NET1 is the external network. As an example, TOE protects NET2 and DMZ from NET1 by properly configuring the gateway between them.

Networks in Figure 1 are as follows:

NET1: Internet

NET2: Local Area Network (LAN)

DMZ: Demilitarized Zone (DMZ)

SECURE ENVIRONMENT: Environment which is probably the server room of the company or institution. Authorized company personnel may access this room but they may be unauthorized to use TOE, which means that they may not be authorized administrator or authorized root administrator of the TOE.

System administrator use **administrator workstation** in secure environment to use TOE. **LMC** (client side of TOE) runs administrator workstation,

Demilitarized Zone is a special intra network, which has server systems on it and it must be protected from other networks. These servers are servicing both the internet and the intranet for different purposes.

Considering this scheme, **LMCS** (server side of TOE) is running Labris Security Gateway Device. Labris Teknoloji also provides the software for installation on Labris compatible third party server hardware. On certification process, TOE is tested only on Labris Security Gateway Device provided by Labris.

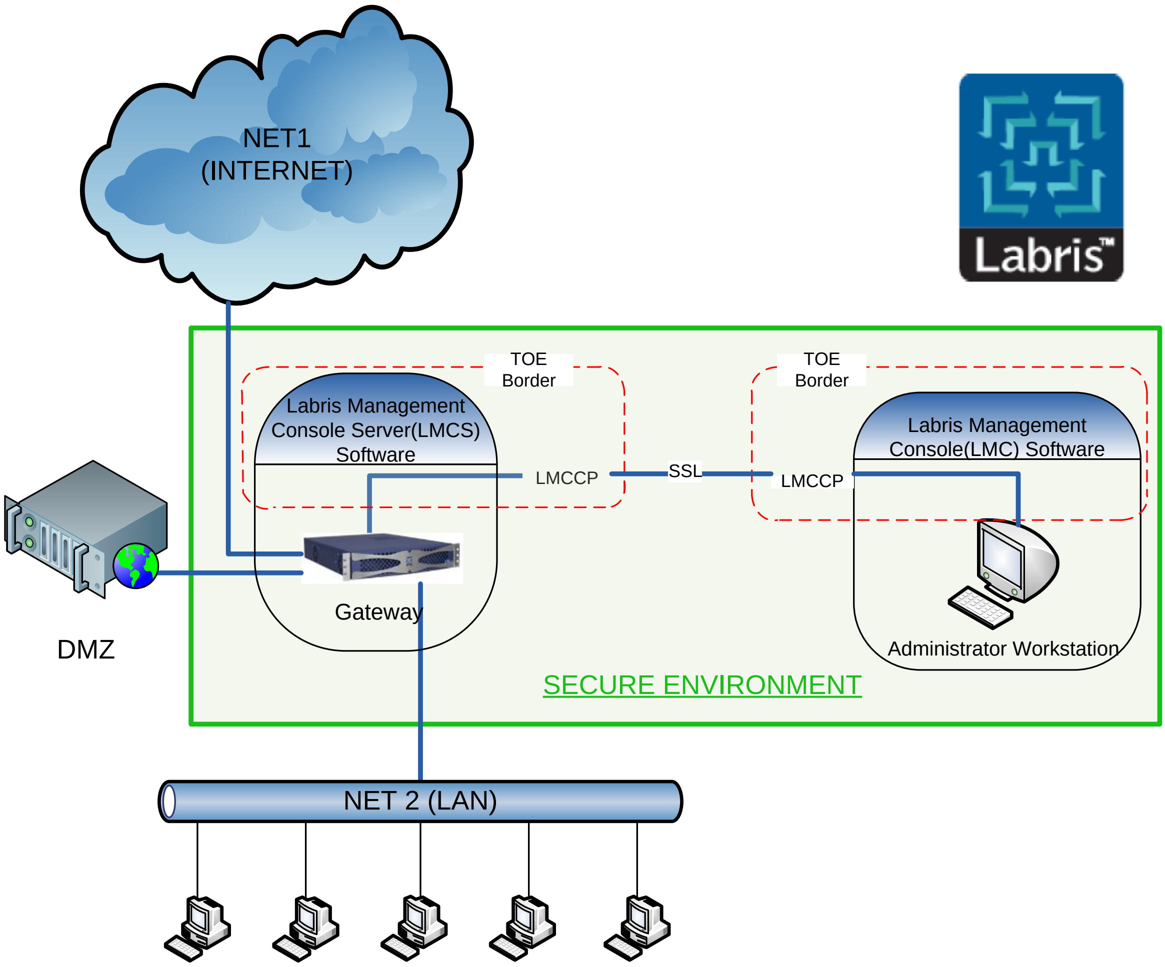

Figure 1 Example Topology

Note: TOE and its execution environment are able to support up to 60000 simultaneous connections (including the connections with the Administrator Workstation) without compromising security and malfunctioning. Connections with the Administrator Workstation have no separate resources allocated to them

1.6.2 Logical Scope

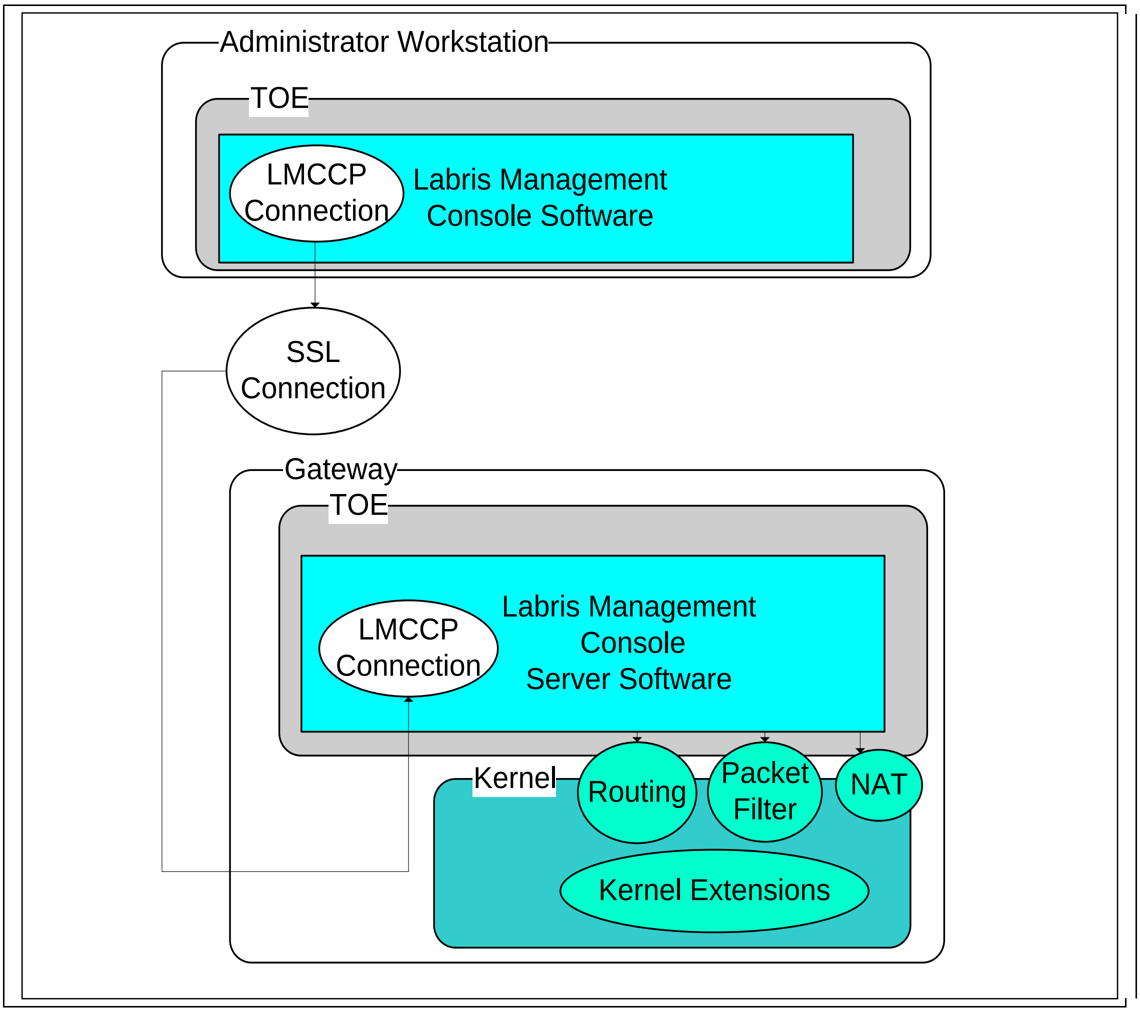

Figure 2 TOE Boundaries

2 CONFORMANCE CLAIM

The conformance claims regarding to the TOE are stated in the following sub-sections.

2.1 CC Conformance Claim

This TOE and ST are consistent with the following specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009, extended.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1, Revision 3, July 2009, augmented.

2.2 PP and Package Claim

2.2.1 Protection Profile (PP) Claim

This ST makes no conformance claims to any certified Protection Profile.

2.2.2 Package Claim

The TOE is conformant to EAL4+ (ALC_FLR.2)

This Security Target elaborated in conformance with “Common Criteria for Information Technology Security Evaluation, Version 3.1 rev 3” contains the IT security requirements of the TOE and specifies the functional and assurance security measures to meet the stated requirements.

2.3 Conformance Rationale

The assurance level of EAL4+ is considered to be most appropriate for this type of TOE since it is intended to defend against attacks that can be made given the assumptions, and the threats defined in chapter 3. Since TOE need continous assurance, package claim for EAL4 is augmented with the component ALC_FLR.2.

3 SECURITY PROBLEM DEFINITION

TOE is intended for use by both commercial and military institutions as well as individual persons who may need protection for their assets. These institutions or individuals have sensitive data that shall be hindered from adversaries, intruders or unauthorized external entities in external network. Sensitive information residing in internal network that is available to authorized LAN users are protected by the proper security policy configuration provided by TOE.

3.1 Assumptions

The following conditions are assumed to exist in the operational environment.

A.CORRECT The platform, where management console runs, correctly transmits the information to the server by direct link, and receives the information correctly, which is sent to it by the server from the same direct link.

A.NOEVIL Authorized root administrator and authorized administrators are non-hostile

A.FOLLOW Authorized administrators and Authorized Root Administrators follow all administrator guidance; however, they are capable of error.

A.PHYSEC TOE is physically secure. It is assumed that there are no physical attacks on platforms where LMC server and LMC client is running. TOE shall only be accessed and managed from a Secure Environment using Management Console monitor, keyboard and mouse. A securely configured Management Console shall be directly connected to the LMC Server via dedicated link entirely within a secure environment.

3.2 Threats

Possible threat agents considered for TOE are unauthorized persons or external IT entities, which are not authorized to use TOE. Threat agents are considered independent entities with a low level of attack sophistication, which are not able to perform organized attacks on TOE.

T.REPEAT An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

T.AUDFUL An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker’s actions.

T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use security function and/or non-security functions provided by the TOE.

T.AUDACC An unauthorized person may not be accountable for the TOE attack actions, because the audit records are not reviewed, thus allowing an attacker to escape detection.

T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data.

3.3 Organizational Security Policies

The following security policies shall be applied by the organization hosting the TOE.

P.GENPUR There shall be no use of general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on platforms where TOE runs.

P.PUBLIC The platforms where TOE runs shall not host public data. Databases or other company related information that may be accessed from internal or external network, which is publicly available to remote applications, shall not be stored on platforms where TOE runs.

P.SINGEN Network infrastructure shall be configured such that all the information between internal networks, external networks and DMZ pass through the gateway configured by the TOE.

4 SECURITY OBJECTIVES

4.1 Security Objectives for the TOE

The following are the IT security objectives for the TOE:

O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.

O.SECFUN The TOE must provide functionality that enables an authorized administrator and authorized root administrator to use the TOE security functions which he is authorized to use, and must ensure that only authorized administrators and authorized root administrators are able to access that authorized functionality.

O.LIMEXT The TOE must provide the means for an authorized administrator and authorized root administrator to control and limit access to TOE security functions by an authorized external IT entity.

O.SELPRO The TOE must protect itself by configuring the IT environment, against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC The TOE must provide a means to access the record of readable audit trail of security related events stored in operating environment, with accurate dates and times, and TOE must provide means to search the audit trail based on relevant attributes using operating environment capabilities.

O.ACCOUN The TOE must provide a means to establish user accountability for information flow through the operating environment. The TOE must generate user accountability information for authorized administrator and authorized root administrator, for their use of security functions related to audit.

4.2 Security Objectives for the Environment

Following objectives shall be met by TOE environment. These are objectives, which shall be satisfied without imposing technical requirements on the TOE.

The following conditions are assumed to exist in the operational environment.

4.2.1 IT Security Objectives for the Environment

OE.SELPRO The operating environment must protect itself and TOE, against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions or security functions provided by operating environment itself.

OE.AUDREC The operating environment must provide an interface to TOE to record a readable audit trail of security related events, with accurate dates and times, and an interface to search the audit trail based on relevant attributes.

OE.ACCOUN The operating environment must provide user accountability for information flows through the operating environment and for authorized administrator and authorized root administrator use of security functions related to audit.

4.2.2 Non-IT Security Objectives for the Environment

OE.CORRECT The platform, where management console runs, shall correctly transmit the information to the server by direct link, and receive the information correctly, which is sent to it by the server from the same direct link. If there is a physical error in the line or if one of the network interface cards used between LMC Server and LMC Client fail, it would not be possible for TOE to behave correctly.

OE.NOEVIL Authorized root administrator and authorized administrators are non-hostile. They shall behave in a correct manner and they shall not aim to attack TOE by any means.

OE.FOLLOW Authorized administrators and Authorized root administrators shall follow all administrator guidance to operate TOE correctly. However, they are capable of error.

OE.PHYSEC TOE, administrative and non-administrative environmental units (except monitor, keyboard and mouse) where LMC Client and LMC Server is running shall be kept in a physically secure container. TOE shall be protected from physical attacks by authorized administrator and authorized root administrator.

OE.GENPUR TOE Environment shall not have general-purpose computing capabilities, which allow installation of non-TOE related software, which may endanger the operation of TOE by preventing trusted execution of the TSF's.

OE.PUBLIC The platforms where TOE runs shall not host public data. Databases or other company related information that may be accessed from internal or external network, which is publicly available to remote applications, shall not be stored on platforms where TOE runs due to threats that can be introduced by access of remote users or applications to TOE hosting platforms.

OE.SINGEN TOE shall be installed according to the following defined firewall architectures. These are bastion host, screened host, multi-homed and screened subnet with n-tier architectures. These architectures ensure that the configured gateway by the TOE is the single point that data must flow through. There must not be covert channels that data can flow from external to internal network or in the opposite direction.

OE.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security. TOE delivery, installation and administration process shall not be compromised or masqueraded by adversaries. Only authorized entities shall deliver, install and operate TOE.

OE.ADMTRA Authorized administrators are trained about the establishment and maintenance of security policies and practices. TOE administrators shall be trained before TOE installation and operation. They shall be informed of all possible configurations and made aware of the network security concepts before operating the TOE. Trainings shall be long enough to cover all topics of the administrative guidance documents.

4.2.3 Security Objectives Rationale for TOE

TOE Security Objectives that are countered to threats are cross-linked in the Table 2. It can be seen from the table that all of the objectives are addressing one or more threats.

	T.NOAUTH	T.AUDACC	T.SELPRO	T.AUDFUL	T.REPEAT
O.IDAUTH	**X**				**X**
O.SELPRO			**X**	**X**	
O.AUDREC		**X**		**X**	
O.ACCOUN		**X**			
O.SECFUN	**X**		**X**	**X**	
O.LIMEXT	**X**		**X**		

Table 2 Mapping of TOE Objectives to Threats

The following is justification for Objectives that are met by TOE.

O.IDAUTH This security objective is necessary to counter the threat T.NOAUTH and T.REPEAT because it requires that users should be uniquely identified and authenticated by TOE before accessing to it.

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL. TOE shall protect itself from attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC This security objective is necessary to counter the threats: T.AUDACC and T.AUDFUL. TOE shall provide a means to record a readable audit trail of security related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC. TOE shall provide user accountability for information flowing through the TOE and for authorized administrator and authorized root administrator use of security functions related to audit.

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH, T.AUDFUL and T.SELPRO. TOE shall provide functionality that enables an authorized administrator and authorized root administrator to use the TOE security functions, and must ensure that only authorized administrators and authorized administrator are able to access such functionality.

O.LIMEXT This security objective is necessary to counter the threats T.NOAUTH and T.SELPRO because the TOE must provide the means for an authorized administrator and authorized root administrator to control and limit access to TOE security functions by an authorized external IT entity.

4.2.4 Security Objectives Rationale for Operational Environment

Environmental Security Objectives that are countered to threats, assumptions and policies are cross-linked in the Table 3. It can be seen from the table that all of the objectives are addressing one or more threats, assumptions or policies

	T.AUDACC	T.NOAUTH	T.SELPRO	A.CORRECT	A.NOEVIL	A.FOLLOW	A.PHYSEC	P.GENPUR	P.PUBLIC	P.SINGEN	T.USAGE
OE.SELPRO		X	X								
OE.AUDREC	X										
OE.ACCOUN	X										
OE.CORRECT				X							
OE.NOEVIL					X						
OE.FOLLOW						X					
OE.PHYSEC							X				
OE.GENPUR								X			
OE.PUBLIC									X		
OE.SINGEN										X	
OE.GUIDAN											X
OE.ADMTRA											X

Table 3 Mapping of Environment Objectives to Threats, Assumptions and Policies

OE.SELPRO This IT security objective is necessary to counter the threats: T.SELPRO and T.NOAUTH. Operating environment shall protect TOE from attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions, by using proper configuration provided by TOE.

OE.AUDREC This IT security objective is necessary to counter the threats: T.AUDACC. Operating environment shall provide an interface for TOE to record a readable audit trail of security related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

OE.ACCOUN This IT security objective is necessary to counter the threat: T.AUDACC. Operating environment shall provide user accountability for information flowing through it and for authorized administrator and authorized root administrator use of security functions related to audit.

OE.CORRECT This non-IT objective is required to cover A.CORRECT. The platform, where management console runs, shall correctly transmit the information to the server by direct link, and receive the information correctly, which is sent to it by the server from the same direct link.

OE.NOEVIL This non-IT objective is necessary to cover A.NOEVIL. Authorized root administrator and authorized administrators are non-hostile. They shall behave in a correct manner and they shall not aim to attack TOE by any means.

OE.FOLLOW This non-IT objective is necessary to cover A.FOLLOW. Authorized administrators and Authorized root administrators shall follow all administrator guidance to operate TOE correctly. However, they are capable of error

OE.PHYSEC This non-IT objective is necessary to cover A.PHYSEC. TOE, administrative and non-administrative environmental units (except monitor, keyboard and mouse) where LMC Client and LMC Server is running shall be kept in a physically secure container.

OE.GENPUR This non-IT objective is necessary to cover P.GENPUR. TOE Environment shall not have general-purpose computing capabilities, which allow installation of non-TOE related software, which may endanger the operation of TOE by preventing trusted execution of the TSF's.

OE.PUBLIC This non-IT objective is necessary to cover P.PUBLIC. The platforms where TOE runs shall not host public data.

OE.SINGEN This non-IT objective is necessary to cover P.SINGEN. IT Environment of TOE shall be the single point that data must flow through. There must not be covert channels that data can flow from external to internal network or opposite direction.

OE.GUIDAN This non-IT security objective is necessary to counter the threat T.USAGE. The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

OE.ADMTRA This non-IT security objective is necessary to counter the threat: T.USAGE .Authorized administrators shall be trained as to establishment and maintenance of security policies and practices. TOE administrators shall be trained before TOE installation and operation. They shall be informed of all possible configurations and made aware of the network security concepts before operating the TOE. Trainings shall be long enough to cover all topics of the administrative guidance documents.

5 EXTENDED COMPONENT DEFINITION

5.1.1 Reliable Time Stamps

The following table contains the extended security functional requirements for the TOE:

Requirement Class	Requirement Components
FPT: Protection of TSF	FPT_STM_EXT.1 Reliable Time Stamps

FPT class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data. This component is a member of FPT_STM, an existing CC Part 2 family. The following extended requirement for the FPT class has been included in this ST because the operational environment is capable of providing reliable time stamps for TSF functions, which is not covered in CC Part 2.

FPT_STM_EXT.1 Reliable Time Stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM_EXT.1.1 The operational environment shall be able to provide reliable time stamps for TSF functions.

Application Note: Reliable Time Stamps is required for the TOE to capture date and time events in relations to the FAU_GEN.1 security functions. The TOE does not have feature to generate time stamps independently. However, the TOE is able to capture the date and time event from the environment which is derived from the Operating System.

6 IT SECURITY REQUIREMENTS

6.1 TOE Security Functional Requirements

This section provides functional and assurance requirements that must be satisfied by TOE. These requirements consist of functional components from Part 2 of the CC and assurance components from Part 3 of the CC.

6.1.1 Overview

The security functional requirements (SFR) for this ST consist of the following components from Part 2 of the CC, summarized in the following Table 4.

Identifier	Name
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behavior
FMT_MOF.1(1)	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles

Table 4 TOE Security Functional Requirements

6.1.2 Security Functional Requirements

6.1.2.1 FAU_GEN.1 Audit data generation [1]

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) [Events specified in Table 5].

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, 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, [information specified in second column of Table 5].

Auditable Event	**Other Audit Relevant Information**
All authentication attempts	submitted user id by the user if authentication is successfull, IP address of the user’s host used for connection, date and time of the event, success or failure of the authentication process
All modifications of the values of security attribute.	Creation of new authorized administrator Deletion of an authorized administrator An authorized administrator or authorized root administrator changes his or her own password Authorized administrator changes the password of an authorized administrator or authorized root administrator. User access level change for an authorized administrator Real name value changed for an authorized administrator or authorized root administrator. Comment value changed for an authorized administrator or authorized root administrator.
Modifications to the group of users that are part of a role;	User access level change for an authorized administrator, new access level, user id
Firewall policy write	Policy name, operation type write
Firewall policy removal	Policy name, operation type remove
Firewall policy installation	Policy name, operation type install

Table 5 Auditable Events by TOE

[1] FPT_STM.1 Time stamps for audit entries are generated by the IT Environment

6.1.2.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [authorized administrators and an authorized root administrator] with the capability to read [all audit trail data] 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.

6.1.2.3 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [*searches*] of audit data based on:

a) [presumed subject address;

b) range of dates;

c) range of times]

6.1.2.4 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] ~~unauthorized~~ modifications to the stored audit records in the audit trail.

6.1.2.5 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [*prevent auditable events, except those taken by the authorized administrator or authorized root administrator* ~~user with special rights~~] and [shall enforce the backup and deletion audit trail] if the audit trail is full.

6.1.2.6 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [ACCESS CONTROL SFP] on [entities defined following table].

Entity	Type	Explanation
Authorized root administrator	subject	He/she is the super user entity who has the all of the available rights defined ACCESS CONTROL SFP and can carry out admin operations. There is only one predefined authorized root administrator, no more authorized root administrator can be added to system and his/her rights can not be lessened.
Authorized administrator	subject	He/she is the user entity who has restricted rights defined in User Attributes Database. He/she cannot have the right to carry out admin operations.
TOE Modules	object	A TOE module is a group of functions, which is used for a specific task. Each TOE module has a name and this name is used to determine if authorized administrator has access to a TOE module function that manipulates ACCESS CONTROL SFP objects.
User Attribute Database	object	User Attribute Database, which stores user id, TOE module name, operation triplet, for each authorized administrator.
Firewall Policies	object	Firewall Policies are information flow policies saved in the internal format of Labris.
LFW Script	object	LFW script is the compiled information flow policies.
Interface Script	object	Interface script is used to manipulate the TOE network interface card configuration.
Log Agent	object	Log agent is a database interface used to access audit trail.
Power	object	Power interface used to start up, shutdown or reboot the Labris OS.
Backup Storage	object	Backup storage is used to access or restore backups.
Date	object	Date is used to change system time of Labris OS.
None	operation	If a TOE module function can be used by an authorized administrator, who has “none” value, defined in User Attribute Database for that TOE module, using this function is a “none” operation.
Read	operation	If a TOE module function can be used by an authorized administrator, who has “read” value, defined in User Attribute Database for that TOE module, using this function is a “read” operation.
Write	operation	If a TOE module function can be used by an authorized administrator, who has “write” value, defined in User Attribute Database for that TOE module, using this function is a “write” operation.
Admin	operation	If a TOE module function can only be used by the authorized root administrator, using this function is an “admin” operation.

6.1.2.7 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 TSF shall enforce the [ACCESS CONTROL SFP] to objects based on the following: [subjects and objects controlled and relevant security attributes defined in Table 6].

Entity	Relevant Security Attributes
Authorized root administrator	For all TOE modules, admin access is granted
Authorized administrator	One of none, read and write accesses for each TOE module are granted.
TOE Modules	Each TOE module requires varying operation accesses to allow use of its various functions depending on the functions nature.
User Attribute Database	Reading User Attributes Database requires read access for System Module. Adding, removing authorized administrators or changing an authorized administrator’s attributes other than passwords requires admin access for System Module. Changing user password of an authorized administrator other than own password requires admin access for System Module. Changing own user password of an authorized administrator requires read access for System Module.
Firewall Policies	Reading Firewall Policies requires read access level for Firewall Module. Saving edited Firewall Policies requires write access level for Firewall Module.
LFW Script	Executing the LFW Script to change information flow control policy of the gateway, which TOE runs requires write access for Firewall Module.
Interface Script	Executing the Interface Script to change information flow control policy of the gateway, which TOE runs, requires write access for IP Route Module.
Log Agent	Reading audit trail via Log Agent requires read access for System Module. Deleting and taking backup of audit trail requires admin access for System Module.
Power	Shutdown and rebooting Labris OS via power interface requires write access for System Module.
Backup Storage	Taking backup or restoring backup requires admin access for authorized administrator.
Date	Reading system date requires read access for System Module. Changing system date requires admin access for System Module.

Table 6 Subjects and objects controlled and relevant security attributes

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) Accessible operation level on an object for subject is determined using the User Attributes Database object. User id of the subject and name of the TOE module, which encapsulates the function that accessing the object, used to find the corresponding operation type.

b) An operation on an object is allowable only if the accessing subject has access to the equal or greater type of operation on the object.

c) Operation access level order from greater to lesser is admin, write, read, none.]

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

a) Authorized root administrator has access to all objects for all operations

b) Authorized root administrator and authorized administrators has access to all objects for operations that require none access level.]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [

a) For all objects, operations that require admin access level are not accessible by the authorized administrators.]

6.1.2.8 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) identity;

b) association of a human user with the authorized administrator role or authorized root administrator role;

c) and an access profile, which identifies the group of access privileges accorded to the user.]

6.1.2.9 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [user identification as stated in FIA_UID.2] 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.

6.1.2.10FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself by entering a username and password on the Management Console GUI before allowing any other TSF-mediated actions that are invoked through Management Console GUI on behalf of that user.

6.1.2.11FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*disable, enable]* the functions:

[a) Permission to reboot and shutdown;

b) Permission to create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) Create, delete, modify, and view user attribute values defined in FIA_ATD.1;

d) Modify and set the time and date;

e) Permission to archive, delete, and review the audit trail;

f) Backup of user attribute values, information flow security policy rules, and audit trail data,

g) Recover to the state following the last backup;]

to [an authorized root administrator].

6.1.2.12FMT_MOF.1 (1) Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*disable, enable]* the functions:

[a) Permission to reboot and shutdown;

b) Permission to create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) View user attribute values defined in FIA_ATD.1;

d) Permission to review the audit trail;

to [an authorized administrator].

6.1.2.13FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [ACCESS CONTROL SFP] to restrict the ability to [*create, modify, delete, view, backup, recover*] the security attributes [defined in FIA_ATD.1.1]to the [authorized administrator or authorized root administrator].

6.1.2.14FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [ACCESS CONTROL SFP] to provide [*restrictive*] default values for ~~security attributes~~ access policy attributes defined in FDP_ACC.1 that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [nobody] to specify alternative initial values to override the default values when an object or information is created.

Application Note: The default values for the attributes appearing in FDP_ACC.1 are intended to be restrictive in the sense that access denied by the TOE until the default values are modified by an authorized administrator or authorized root administrator. For example, default operation level for created authorized administrator entities is lowest available operation level for all modules, which prevents authorized administrator to do any actions until authorized root administrator grants higher access.

6.1.2.15FMT_SMF.1 Specification of Management Functions

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

a) Reboot and shutdown

b) create, delete, modify, and view information flow security policy rules that permit or deny information flows.

c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;

d) modify and set the time and date;

e) archive, create, delete and review the audit trail;

f) backup of user attribute values, information flow security policy rules, and audit trail data and

g) recover to the state following the last backup]

6.1.2.16FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [authorized administrator and authorized root administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with authorized administrator and authorized root administrator roles.

6.1.3 Security Functional Requirements Rationale

Rationale for security TOE functional requirements are shown in Table 7. In this table, security objectives and security functional requirements are cross-linked and their dependency is shown.

	O.IDAUTH	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FAU_GEN.1			X	X		
FAU_SAR.1			X			
FAU_SAR.3			X			
FAU_STG.1		X			X	
FAU_STG.4		X			X	
FDP_ACC.1		X			X	
FDP_ACF.1		X			X	
FIA_ATD.1	X			X		
FIA_UID.2	X	X				
FIA_UAU.1	X	X				
FMT_MSA.1	X				X	
FMT_MSA.3	X				X	
FMT_MOF.1					X	X
FMT_MOF.1(1)					X	X
FMT_SMF.1					X	X
FMT_SMR.1					X	

Table 7 Rationale for TOE Security Functional

FAU_GEN.1 Audit data generation

This component defines requirements to identify the auditable events for which audit records shall be generated, and the information to be provided in the audit records. O.AUDREC and O.ACCOUN objectives are in the scope of this component.

FAU_SAR.1 Audit review

This component ensures that the audit trail is understandable. This component traces back to and helps meeting the objective O.AUDREC.

FAU_SAR.3 Selectable audit review

This component ensures that a variety of searches can be performed on the audit trail. This component traces back to and aids in meeting the objective O.AUDREC.

FAU_STG.1 Protected audit trail storage

This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the objectives O.SELPRO and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

This component ensures that the authorized administrator or authorized root administrator will be able to take care of the audit trail if it becomes full. However, this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus authorized administrator and authorized root administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the objectives O.SELPRO and O.SECFUN.

FDP_ACC.1 Access control subset

This exists to define subjects, objects and operations of ACCESS CONTROL SFP. This component traces back to and aids in meeting the objectives O.SELPRO and O.SECFUN.

FID_ACF.1 Security based access control

This exists to describe the rules of ACCESS CONTROL SFP. This component traces back to and aids in meeting the objectives O.SELPRO and O.SECFUN.

FIA_ATD.1 User attribute definition

This component exists to set user attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the objectives O.IDAUTH and O.ACCOUN.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of a user, user's identity is identified to the TOE. This component traces back to and aids in meeting the objective O.IDAUTH and O.SELPRO.

FIA_UAU.1 Timing of authentication

This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator or authorized root administrator. If the authorized administrator or authorized root administrator were not always required to authenticate, there would be no means by which to audit any of their actions. An additional SOF metric for this requirement is defined in section 5.3 to ensure that the authentication mechanism chosen cannot be easily bypassed. This component traces back to and aids in meeting the objective O.IDAUTH and O.SELPRO.

FMT_MSA.1 Management of Security Attributes

This component requires TSF to allow authorized administrators and authorized root administrator to manage the specified security attributes and aided in meeting the objectives O.IDAUTH and O.SECFUN

FMT_MSA.3 Static attribute initialization

This component ensures that there is default "none" access level for authorized administrators. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.

FMT_MOF.1 Management of security functions behavior

This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate authorized administrator related TOE management/administration/security functions. This component traces back to and aids in meeting the objectives O.SECFUN, O.LIMEXT.

FMT_MOF.1 (1) Management of security functions behavior

This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate authorized administrator related TOE management/administration/security functions. This component traces back to and aids in meeting the objectives O.SECFUN, O.LIMEXT.

FMT_SMF.1 Specification of Management Functions

This component ensures presence of specific management functions provided by TSF and aided in meeting the objectives O.SECFUN and O.LIMEXT

FMT_SMR.1 Security roles

Each of the CC class FMT components in this ST is dependent to this component. This component aids in meeting the objective: O.SECFUN.

6.1.4 Rationale for Dependencies

Table 8 shows the TOE Security Functional Requirements and associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components, which are hierarchical to the specified dependency

Security Functional Requirement	Dependencies	Dependency Satisfied	Notes
FAU_GEN.1	FPT_STM.1	Yes	FPT_STM.1 dependency is satisfied by TOE Security Environment
FAU_SAR.1	FAU_GEN.1 FAU_GEN.1 (1)	Yes Yes	FAU_GEN.1 (1) dependency is satisfied by TOE Security Environment
FAU_SAR.3	FAU_SAR.1	Yes	-
FAU_STG.1	FAU_GEN.1 FAU_GEN.1 (1)	Yes Yes	FAU_GEN.1 (1) dependency is satisfied by TOE Security Environment
FAU_STG.4	FAU_STG.1	Yes	-
FDP_ACC.1	FDP_ACF.1	Yes	-
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes	-
FIA_ATD.1	None	N/A	-
FIA_UAU.1	FIA_UID.1	Yes	FIA_UID.2 is hierarchical to FIA_UID.1
FIA_UID.2	None	N/A	-
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Yes Yes	-
FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	Yes Yes	-
FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	Yes Yes Yes	-
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes	-
FMT_SMF.1	None	N/A	-
FMT_SMR.1	FIA_UID.1	Yes	FIA_UID.2 is hierarchical to FIA_UID.1

Table 8 TOE Functional Requirement Dependencies Rationale

6.2 TOE Security Assurance Requirements

6.2.1 List of Assurance Requirements

The security assurance requirement level is EAL 4 augmented (ALC_FLR.2). Assurance requirements for this ST are taken from Part 3 of the CC.

The assurance components are summarized in the following Table 9:

Assurance Class	Assurance Components	
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 Specifications
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete Functional Specification
	ADV_IMP.1	Implementation Representation of the TSF
	ADV_TDS.3	Basic Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and Automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.2 (+ requirement)	Flaw Reporting Procedures
	ALC_LCD.1	Developer Defined Life Cycle Model
	ALC_TAT.1	Well Defined Development Tools
Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing-sample
Vulnerability Assessments	AVA_VAN.3	Focused Vulnerability Analysis

Table 9 TOE Security Assurance Requirements

6.2.2 Security Assurance Requirements Rationale

EAL 4+ (ALC_FLR.2) was chosen to provide a methodically designed tested and reviewed frame for TOE evaluation. EAL 4 permits a developer to gain moderate level assurance from positive security engineering based on good commercial development practices, which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is probably the highest level where retrofitting an existing product line is economically feasible.

Higher assurance levels than EAL 4 requires semiformal or formal representations. Applications related to network perimeter security are too complex and have multiple parts and interfaces, which are very expensive to explain formally or semi-formally. Almost all of the CC evaluated competitive products, which are in the same domain with TOE; provide equal or lower assurance level for reasons stated above. TOE assurance level EAL 4+ (ALC_FLR.2) is sufficient for identified objectives, threats and proposed TOE usage.

Labris Teknoloji claims that the TOE complies to EAL 4 augmented with ALC_FLR.2 and is resistant to threats that may be originated from subjects that are sending or receiving information through TOE even in case of independent vulnerability assessment analysis.

7 TOE Summary Specification

In this section, TOE Security Functions and TOE Assurance Measures are explained. These functions and assurance measures are cross-referenced with functional requirements and assurance requirements respectively in Rationale Section.

7.1 TOE Security Functions

TOE Security Functions is demonstrated in Table 10.

F.MMI	Authorized root administrator can manage security with Man Machine Interface functions explained below, which can be accessed from management console: a) Reboot and shutdown; b) create, delete, modify, and view information flow security policy rules that permit or deny information flows; c) create, delete, modify, and view user attribute values defined in FIA_ATD.1 • Identity • Association of a human user with the authorized administrator or authorized root administrator role • Access profile, which identifies the group of access privileges according to the user. d) modify and set the time and date; e) archive, delete, and review the audit trail; f) backup of user attribute values and audit trail data, where the backup capability shall be supported by automated tools; and g) recover to the state following the last backup. Authorized administrator can manage security with Man Machine Interface functions explained below of which can be accessed from management console: a) Reboot and shutdown; b) create, delete, modify, and view information flow security policy rules that permit or deny information flows; c) view user attribute values defined in FIA_ATD.1 • Identity • Association of a human user with the authorized administrator or authorized root administrator role • Access profile, which identifies the group of access privileges accorded to the user. d) review the audit trail;
F.AUDLOG	TOE is capable of generating logs for events explained below a) Start-up and shutdown of the audit functions; and b) All auditable events specified in Table 5.

F.AUDDET	TOE has minimal audit log detail. Entries explained below exist in TOE for each audit log event. a) Date and time of the event; b) type of event; c) subjects' identities; d) outcome [success or failure] of the event; and e) for each audit event type, based on the auditable event definitions of the functional components included in the ST, the information specified in second column of Table 3.

F.AUDLST	Authorized administrator and authorized root administrator can access TOE audit trails and TOE Security Environment audit trails. He can perform search among logged entries according to following log entry properties.
	a) presumed subject address;
	b) ranges of dates;
	c) ranges of times;

F.AUDPROT	TOE has the capability of protecting audit data from modification or deletion. Loss of audit data is protected by TOE by stopping the events that create audit logs except actions performed by authorized administrator or authorized root administrator. When audit trail storage is at its defined limits. TOE enforces authorized root administrator to backup audit trail for TOE to continue functioning properly.
F.ADMIN	Only authorized administrators and authorized root administrators, who use a management console, which operates in secure environment, can access TOE. Authorized administrators have their own privileges that are set by authorized root administrator.
F.IDAUTH	Authorized administrators and authorized root administrators shall first identify and authorize themselves to TOE before doing any operation on TOE. Probability that authentication data can be guessed is smaller than 0.000001.
F.DEFVAL	Security attributes that are used to enforce TOE SFP's have restrictive initial values. Authorized administrators and authorized root administrators can override these default values by editing object properties after new information flow policy object or authorized administrator entity is created.

Table 10 TOE Security Functions

7.2 TOE Security Functions Rationale

Table 19 provides a bi-directional mapping of Security Functions to Security Functional Requirements. It shows that each SFR is addressed by at least one of the Security Functions and that each of the Security Functions addresses at least one of the SFR' s. The table is followed by a discussion of how each security functional requirement is addressed by the corresponding security function.

	FAU_GEN.1	FAU_SAR.1	FAU.SAR.3	FAU_STG.1	FAU_STG.4	FDP_ACC.1	FDP_ACF.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.2	FMT_MOF.1	FMT_MOF.1(1)	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1
F.MMI								X			X	X			X	X
F.AUDLOG	X															
F.AUDDET	X															
F.AUDLST		X	X													
F.AUDPROT				X	X											
F.ADMIN						X	X	X								X
F.IDAUTH						X	X		X	X						
F.DEFVAL													X	X		

Table 11 TOE Security Functions Rationale

FAU_GEN.1[2] F.AUDLOG, F.AUDDET combines to satisfy the requirement for the generation of audit data for the predefined set of TOE events. F.AUDLOG generates log and F.AUDDET provides appropriate entries [2]

FAU_SAR.1 Requirement of providing audit data to authorized administrator in a manner that permits interpretation is accomplished by F.AUDLST.

FAU_SAR.3 Providing audit review mechanism to select the audit data to be reviewed based on defined criteria requirement is satisfied by F.AUDLST.

FAU_STG.1 F.AUDPROT satisfies the requirement for protected storage of audit trails by preventing audit data modification or deletion by unauthorized users.

FAU_STG.4 F.AUDPROT provides the mechanism for the requirement to protect stored audit data and to prevent data loss if the audit trail is full.

FDP_ACC.1 F.IDAUTH function requires authentication before allowing any other TSF-mediated actions on behalf of the administrator to allow enforcing of ACCESS CONTROL SFP according to user id. F.ADMIN provides access levels for authorized root administrator and authorized administrators.

[2] Use of reliable time stamps is also necessary to fully satisfy this requirement, but this is supplied from the environment, which is operating system (Labris OS) that TOE runs

FDP_ACF.1 F.IDAUTH function requires authentication before allowing any other TSF-mediated actions on behalf of the administrator to allow enforcing of ACCESS CONTROL SFP according to user id. F.ADMIN provides access levels for authorized root administrator and authorized administrators.

FIA_ATD.1 F.ADMIN satisfies the requirement to maintain a list of security attributes belonging to individual authorized administrators. F.MMI provides user interfaces for user attribute definition and manipulation.

FIA_UAU.1 F.IDAUTH satisfies the necessary functionality for the requirement to allow identification of the authorized administrator and authorized root administrator before authentication. F.IDAUTH function also requires authentication before allowing any other TSF-mediated actions on behalf of the administrator.

FIA_UID.2 F.IDAUTH satisfies the requirement for each authorized administrator and authorized root administrator to identify itself before allowing any other TSF-mediated actions on behalf of that administrator.

FMT_MOF.**1** F.MMI provides functionality that meets requirement for the TOE to provide the authorized root administrator with the capability to manage the security functions of the TOE through external interfaces.

FMT_MOF.1 (1) F.MMI provides functionality that meets requirement for the TOE to provide the authorized administrator with the capability to manage the security functions of the TOE through external interfaces.

FMT_MSA.1. F.DEFVAL provides functionality for restricted default values.

FMT_MSA.3. F.DEFVAL provides functionality for overriding default values.

FMT_SMF.1 F.MMI provides user interfaces for authorized root administrator and authorized administrator for managing the TOE security management functions.

FMT_SMR.1 F.MMI satisfies the requirement for a TOE to maintain security administration role and associate it with a human user. F.ADMIN provides access levels for authorized root administrator, authorized administrators, which are used to define specific roles for authorized administrators, and authorized root administrator.

8 APPENDIX

8.1 Abbreviations & Glossary

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ST	Security Target
SFR	Security Functional Requirements
SOF	Strength of Function
TOE	Target of Evaluation
TSF	TOE Security Functions
IT	Information Technology
PP	Protection Profile
SFP	Security Function Policy
TSC	TSF Scope of Control
TSP	TOE Security Policy
MMI	Man Machine Interface

Table 12 Abbreviations and glossary

Firewall: It is an IT security device, which is configured to permit, deny, or proxy data connections set and configured by the organization’s security policy.

User: It is any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Human user: He or she is any person who interacts with the TOE.

External IT entity: Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Role: It is a predefined set of rules establishing the allowed interactions between a user and the TOE.

Identity: A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Authentication data: Information used to verify the claimed identity of a user.

Authorized external IT entity: It is any IT product or system, outside the scope of the TOE that may administer the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to, not compromise the security policy enforced by the TOE.

Attack Potential: Potential for success of an attack depending on attacker’s expertise, resources and motivation.

Authorized Root Administrator: Authorized administrator with maximum privileges of TOE security functions. He or she is allowed to give or take permission to Authorized Administrators. Single Authorized Root Administrator role can be defined for single TOE.

Authorized Administrator: Authorized Administrator created by Authorized Root Administrator with privileges specified by Authorized Root Administrator.

LMC: Labris Management Console

LMCS: Labris Management Console Server

LMCCP: Labris Management Console Connection Protocol