Huawei UDG V100R001C20SPC300 with Patch V100R001C20SPH333 Security Target

Version: V2.9 Date of issue: 2022-10-24

Author: Huawei Technologies Co., Ltd.

Table of Contents

List of figures

List of tables

Revision History

Date	Revision Version	Change Description	Author
2019-01-25	V1.3	draft ST	Huawei
2019-10-22	V1.4	Update ST	Huawei
2020-06-17	V1.6	Update ST	Huawei
2020-08-12	V1.7	Update ST	Huawei
2021-06-18	V2.1	Update ST	Huawei
2021-10-27	V2.2	Initial version for evaluation 2021	Huawei
2021-11-26	V2.3	Remove objective O.TIME, add assumption A.TIME and operational environment OE.TIME. Remove control plane and user plane concept and related description. Remove objective O.ENCRYPT, merge this function to O.COMMUNICATION. Correct according to comments.	Huawei
2022-01-11	V2.4	Correct according to OR 025-029	Huawei
2022-01-21	V2.5	Add more SFRs, FCS	Huawei
2022-02-10	V2.6	Correct SFRs FCS class, and update Figure 1, add user role: visit-ug	Huawei
2022-06-17	V2.7	remove SFRs FCS class, and update Figure 1, modify SFR rational	Huawei
		correct OR 025, 028, and issue found by testing	
		correct SFR FDP_ACF.1, and issue found by testing, remove command ‘set WebLMT server parameters’ from system-ug Update U2000 to U2020	
		Add TOE patch in physical scope in section 1.4.1 Add condition for system-ug and monitor-ug to query user data.	
		Add guidance document download link and hash value of this published version, in section 1.4.1	
		Add application note for FTA_MCS.1/WebLMT	
		Correct statement for FIA_AFL.1	
		Remove SSH as the communication security function	
2022-06-30	V2.8	Add TOE patch file and hash value Add SFR FTP_ITC.1 to cover SSH communication security function	Huawei

1 INTRODUCTION

This section contains the ST reference, TOE reference, TOE overview and TOE description of **Huawei UDG**.

1.1 ST REFERENCE

This ST is uniquely identified as below,

Title: Huawei UDG V100R001C20SPC300 with Patch V100R001C20SPH333 Security Target

Version: V2.9

Author: Huawei Technologies Co., Ltd.

Publication date: 2022-10-24

1.2 TOE REFERENCE

The TOE is identified as below,

TOE name: Huawei UDG

TOE version: V100R001C20SPC300 with Patch V100R001C20SPH333

Developer: Huawei Technologies Co., Ltd.

1.3 TOE OVERVIEW

1.3.1 TOE type

The TOE is server service software that is deployed on CloudOS.

The TOE supports GPRS, UMTS, LTE and 5G NSA that comply with 3GPP specifications. It also supports WLAN and NB-IoT services. In addition, it provides service functions of the GGSN, S-GW, P-GW, centralized gateway (CGW), distributed gateway (DGW), meeting various networking requirements of different carriers in different phases and operating scenarios.

1.3.2 TOE usage and major security features

1.3.2.1 TOE Usage

In this section, the usage and its major security features are summarised, TOE type and major non-TOE hardware/software/firmware required by the TOE are summarised.

The UDG, a unified packet gateway independently developed by Huawei, can be used in GPRS, UMTS, LTE, and 5G NSA. The UDG can behaviour as a gateway GPRS support node (GGSN), centralized gateway (CGW), distributed gateway (DGW), serving gateway (S-GW), PDN gateway (P-GW), or any combination of these five roles, and can be managed individually.

The TOE is connected to WebLMT through TLS and U2020 server through SSH. The TOE and its environment are shown in Figure 1 TOE and its environment.

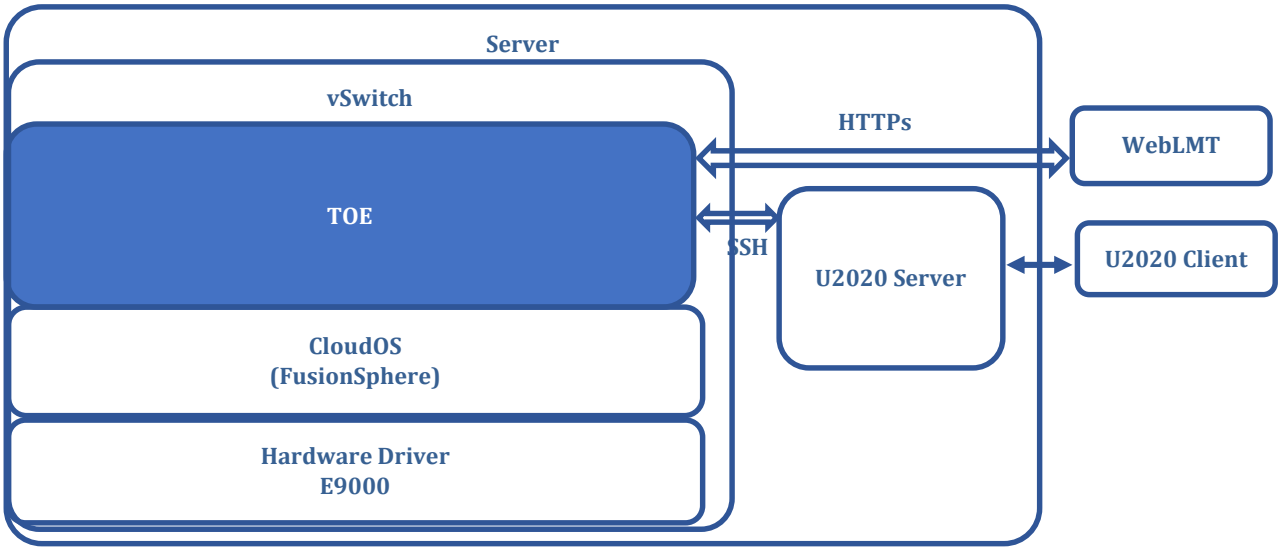


Figure 1 TOE and its environment

1.3.2.2 TOE major security features

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

Auditing

The TOE generates audit records for security-relevant management actions. The audit data can be queried by the authorized user. The TOE classifies the audit record into 2 categories according to the management scope and action: Operation logs, Security logs.

Communications security

The TOE provides communication security by implementing Secure Shell (SSH) and Transport Layer Security (TLS).

The TOE offers TLS encryption for communication between the WebLMT and the TOE, SSH encryption between the U2020 server and the TOE.

Authentication

The TOE authenticates its administrative users (referred as “users” hereafter) via individual usernames and passwords and grant different privileges to the user. The TOE is able to enforce password policies as well as “lockout” policies to defence password brute force attacks. Further, it is possible to limit login of specific users to specific time frames and define expiry dates for accounts and passwords. The user with different privileges can access different command groups and perform different functions. The TOE can detect unsuccessful authentication attempts, and lockout the account if the attempts is met to the maximum number of failure attempts.

Access control

The TOE can limit the session establishment via SSH/TLS using the blacklist/whitelist feature by matching the resource of the session establishment request against the blacklist/whitelist specified. The TOE can limit the user access to the TOE device or application using the ACL (Access Control List) feature by matching IP address and blacklist against ACL rules specified.

Security management

The following means are provided by the TOE for management of security functionality:

- User and group management
- Configuration of TLS/SSH for communications security
- Security role configuration

1.3.3 Non-TOE Hardware and Software

The TOE is UDG software package which supports GPRS, UMTS, LTE or 5G NSA. It is deployed on CloudOS, while the platform is running on hardware boards. These hardware boards are TOE environment. The Cloud OS software are provided by Huawei and are part of the environment.

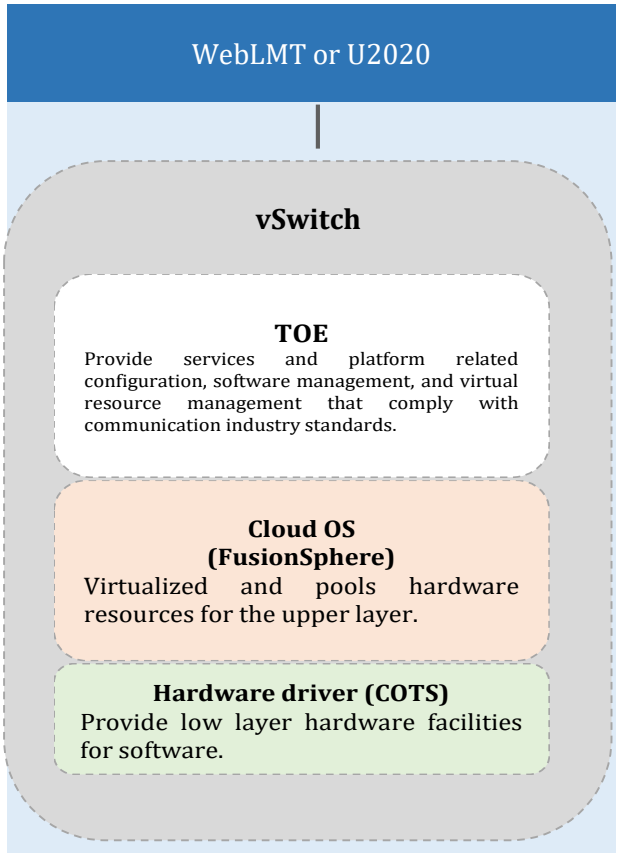


Figure 2 Hardware and Software

Table 1 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Hardware layer	Required	The TOE runs on these hardware platforms. Infrastructure can be Huawei E9000 or RH2288H

Component	Required	Usage/Purpose Description for TOE performance
Cloud OS	Required	The cloud OS provides virtual resources and can be a Huawei FusionSphere
vSwitch	Required	Virtual switch (vSwitch) provides connectivity between Cloud OS and WebLMT.
WebLMT	Required	The WebLMT is used to perform configuration and user management through TLS. The WebLMT has 3 different security user groups which can access different security functions.
U2020 server	Required	Huawei U2020 server supports the functions including configuration and user management via SSH. U2020 server to access TOE, has only one user, which is in the ems-ug.

Note: The TOE environment components are not evaluated given that they are not part of the TOE and therefore there is no assurance regarding these components.

1.3.4 Non evaluated security features

Beside evaluated TOE is also capable to manage mobile subscribers, restrict mobile subscribers to access network by data usage or mobile subscribers' data plan, manage IP protocol processing, routing management, and packet forwarding, and data storage, data backup, and data pushing required by telecommunication services.

In addition, it provides service functions of gateway GPRS support node (GGSN), centralized gateway (CGW), distributed gateway (DGW), serving gateway (S-GW), PDN gateway (P-GW), meeting various networking requirements of different carriers in different phases and operating scenarios, which is using IPSec and TCP/IP protocols to provide data transmission protocol.

But these functions are out of the scope, out of the TSF defined in section 6 TOE Summary Specification. The TSF only include auditing, communication security, authentication, access control and security management functionalities.

1.4 TOE DESCRIPTION

1.4.1 Physical scope of the TOE

The release package for UDG is composed of software and documents. The UDG software package is in the form of binary compressed file.

The TOE base version, the signature file and its guidance documents can be downloaded from the Huawei's support website:

https://support.huawei.com/carrier/navi?coltype=software#col=software&detailId=PBI1-250548962&path=PBI1-21262245/PBI1-7899527/PBI1-22892303/PBI1-252303719/PBI1-22609856

The TOE patch version, the signature file and its guidance document can be downloaded from:

https://support.huawei.com/carrier/navi?coltype=software#col=software&from=product&detailId=PBI1-252597313&path=PBI1-21262245/PBI1-7899527/PBI1-22892303/PBI1-23710417/PBI1-22609856

To download the software, the user(s) need to have a Huawei account of the support website first, and please register an account role with download permission. To obtain a register account, the user(s) have to contact Huawei Customer Service via email (e.support@huawei.com)

The list of the files and documents required for the products is shown as following, in Table 2.

Table 2 Physical Scope

Software and Documents	Description	File type	SHA256
UDG-Option3_V100R001C20SPC300_Install.zip	Base software package (In the form of binary compressed files).	Software	7a4e1c89755051437900ea00e974fc678093c6705a22b797b342ccb953fd759f
UDG-Option3_V100R001C20SPC300_Install.zip.asc	Signature file of base software package	Signature file	b226452291e7e503dc24dc727d166c53a9c8f01840e1386c4aa29b0e11ce8518
UDG-Option3_V100R001C20SPH333.zip	Patch software package	Software	7f002bfa9f4e3b0efe361f772e03a2a93d36e0ee389a4ea92401688146ceceb1
UDG-Option3_V100R001C20SPH333.zip.asc	Signature file of patch software package	Signature file	9c88b15914cd09b2311626bbac5a6185ef6937280e66f3342074b6aa801333d2
Huawei UDG V100R001C20SPC300 With Patch V100R001C20SPH333 Security Management Guide V2.0.pdf	The guidance documents of TOE	Document	5fdf240b6ad3c788e6f4c2f45565efe0593123f5eed3268752285846852884432
Huawei UDG V100R001C20SPC300 With Patch V100R001C20SPH333 Installation Guide V2.0.pdf		Document	4b106c812c29e627dae062159c9c48db9749bb35c14dc399d6eabfd606e5a178
Huawei UDG V100R001C20SPC300 With Patch V100R001C20SPH333 MML Commands Guide, part 1.pdf		Document	95bc31449d5ce82728adb242ec80013f87e2bd47b71bb1e04e961cfa8ac8e2a1
UDG V100R001C20SPC300 Upgrade Guide 07 (CGW, FusionSphere, Upgrade by Using the WebLMT).doc	TOE base version full installation guide (for Huawei engineer only)	Document	0890dfd663cc7f9bcab5646f09c99b329b8cb1ed9a22abf966a68530a8d65f05

Software and Documents	Description	File type	SHA256
UDG V100R001C20SPH333 Upgrade Guide 02 (Upgrade by Using the WebLMT).doc	TOE patch version full installation guide (for Huawei engineer only)	Document	1935b883f37c0383400fde2d9912d3c97f98cfd72ad66965581dca9192e754e0

1.4.2 Logical scope of the TOE

The TOE is composed of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

(1) Auditing

- The log module of the host software records operations on a device and events that occur to a device. The recorded operations and events are log messages. Log messages provide evidence for diagnosing and maintaining a system. Log messages reflect the operating status of a device and are used to analyse the conditions of a network and to find out the causes of network failure or faults.
- The log records user operations, user management, security policy configuration, system management, etc.
- 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.
- Only authorized users can view logs and users can select the log based on the time range and security level.
- The oldest log files will be deleted if the audit trail exceeds the size of store device.

(2) Communication security

- The TOE supports the trusted connections using TLS for the communication with the WebLMT.
- The TOE supports the trusted connections using SSH for the communication with the U2020 server.

(3) Authentication

- The TOE supports one kind of authentication which is user authentication
- The TOE can authenticate users by username and password.
- The TOE can grant different privileges to the user according to user roles.
- The TOE can enforce user password policy.
- In order to protect the TOE, the TSF can restrict the maximum number of concurrent sessions and can lock an interactive session after a time interval. The user should re-authentication prior to unlocking the session.
- The TOE can manage user authorities to ensure that only authorized users are allowed to operate the TOE.
- The TOE can lock the user account for 5 minutes, if this user has 3 unsuccessful authentication attempts within 5 minutes.

(4) Access control

- The TOE supports IP-based Access Control List (ACL) to filter traffic destined to TOE to prevent

internal traffic overload and service interruption.

- The TOE can limit the session establishment via SSH/TLS by blacklist/whitelist filtering, which compares the client of session establishment request with specified blacklist/whitelist. The TOE can reject the session establishment from the IP address in the blacklist, while accept the session establishment request from the IP address or in the whitelist.

(5) Secure Management

- The security management function of the TOE supports user and group management, security role configuration, and secure transmission for TLS and SSH configuration.

1.4.3 Evaluated configuration

The TOE (Huawei UDG version V100R001C20SPC300 with Patch V100R001C20SPH333) runs on a CloudOS, which is running on hardware platform, while the hardware platform is E9000, and the CloudOS is Huawei FusionSphere.

The following table defines all items involved in the TOE evaluated configuration:

Item	Item type	Requirement
TOE	TOE	Huawei UDG version V100R001C20SPC300 with Patch V100R001C20SPH333
Browser	Microsoft Internet Explorer Firefox Google Chrome	Microsoft Internet Explorer 11 Firefox 64.X Google Chrome 55.X
Cloud OS	Fusion Sphere	Version HUAWEI Cloud Stack NFVI 6.5.1
vSwitch	Virtual switch	N/A
Server	E9000	Version: E9000 Chassis V100R001C10SPC522 RAM: 1113GB Hard disk: 6482GB
U2020 Server	Server application run on E9000	Version U2020 V300R019C10SPC540

2 CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

This ST and the TOE conform to the version of CC as below:

Part 1: Introduction and general model Version 3.1 Revision 5

Part 2: Security functional components Version 3.1 Revision 5

Part 3: Security assurance components Version 3.1 Revision 5

This ST conforms to CC Part 2 conformant.

This ST conforms to CC Part 3 conformant.

This ST is EAL4 conformant as defined in [CC] Part 3, with the assurance level of EAL4 Augmented with ALC_FLR.1.

3 SECURITY PROBLEM DEFINITION

The security problems addressed by the TOE and the operational environment of the TOE are defined in this section. Security problem definition shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two.

3.1 THREATS

3.1.1 Assets

The classification of the different data types is given in the following:

- **User Data**: The TOE provides the secure communication service for the TOE users. The user data includes:
  - user identifier
  - user password
  - user security attribute
- **Audit Logs**: The TOE stores audit logs for security events.
- **SSH configuration parameters**: The TOE stores SSH configuration parameters for SSH secure channel establishment:
  - ACL rule name for SSH protocol
  - SSH server encryption algorithm
  - SSH server HMAC algorithm
  - SSH server key exchange algorithm
  - Session management configuration parameters
- **TLS configuration parameters**: The TOE stores TLS configuration parameters for HTTPs secure channel establishment:
  - TLS cipher suite
  - ACL rule name for HTTPs protocol
  - TLS version
- **Access control list**: The TOE stores ACL rule group and rule to restrict session establishment.
  - ACL rule name and rule group name
  - IP address
  - blacklist

3.1.2 Threat Agents

The assets are threatened by the following threat agents:

TA.NETWORK_M:

An attacker who can access the management network that the TOE is connected to.

3.1.3 Threat

The combination of assets and threat agents gives rise to the following threats:

3.1.3.1 Communication Between Network Devices

T.UNAUTHORIZED_ ADMINISTRATOR_ACCESS	
Attack	Attackers disguise as device administrator to read personal communication data or steal system configuration information.
Asset	Confidentiality of the User data, audit logs, SSH configuration parameters, TLS configuration parameters, access control list
Agent	TA.NETWORK_M

T.WEAK_CRYPTOGRAPHY	
Attack	Attackers can obtain keys by brute force cracking to read and control network traffic without authorization.
Asset	Confidentiality of the User data, audit logs, SSH configuration parameters, TLS configuration parameters, access control list
Agent	TA.NETWORK_M

T.UNTRUSTED_COMMUNICATION_CHANNELS	
Attack	Attackers gain access to the connection between TOE and WebLMT or connection between TOE and U2020 server, threatening the integrity and confidentiality of transmitted assets of the TOE.
Asset	Confidentiality and integrity of all these data in transmit: user data, audit logs, SSH configuration parameters, TLS configuration parameters, access control list
Agent	TA.NETWORK_M

T.WEAK_AUTHENTICATION_ENDPOINTS	
Attack	Attackers disguise as a device connected to the TOE, which poses a security threat to network traffic.
Asset	Confidentiality of all these data in transmit: user data, audit logs, SSH configuration parameters, TLS configuration parameters, access control list
Agent	TA.NETWORK_M

3.2 OSP

3.2.1 OSP.AUDIT

The TOE shall generate audit record of security events and operational events.

3.3 ASSUMPTIONS

This section describes the assumptions made in identification of the threats and security requirements for network devices. The network device is not expected to provide assurance in any of these areas, and as a result, requirements are not included to mitigate the threats associated.

3.3.1 A.PHYSICAL_PROTECTION

The TOE, CloudOS, U2020 server and the hardware driver are assumed to be located in a physically protected environment which is protected against unauthorized physical access. Only trusted users are allowed to access it. Communication between the TOE and the U2020 server is physically isolated by using an ethernet cable connecting the two endpoints.

3.3.2 A.LIMITED_FUNCTIONALITY

The hardware, CloudOS and U2020 server, where the TOE is installed, is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing.

3.3.3 A.TRUSTED_ADMINISTRATOR

The security administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are assumed to ensure passwords/credentials are set with sufficient strength and without lack malicious intent when administering the device.

3.3.4 A.ADMIN_CREDENTIALS_SECURE

Administrator's credentials (private key) used to access the network device are assumed to be protected by the platform on which they reside.

3.3.5 A.COMPONENTS_RUNNING

Administrator is assumed to ensure that all of TOE components, which is including the hardware driver layer, and hardware, run correctly.

3.3.6 A.RESIDUAL_INFORMATION

It is assumed that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.3.7 A.NETWORK_SEGREGATION

It is assumed that the TOE is isolated based on proper configurations.

3.3.8 A.TIME

It is assumed that the TOE environment (CloudOS) can provide reliable timestamps to TOE.

3.3.9 A.ENVIRONMENT_ACL

It is assumed that the TOE environment (virtual vSwitch) can provide external access only to the TOE interfaces.

4 SECURITY OBJECTIVES

The security objectives are divided into two solutions. These solutions are called the security objectives for the TOE and the security objectives for the operational environment. It reflects that these solutions are provided by two different entities: the TOE, and the operational environment.

4.1 SECURITY OBJECTIVES FOR THE TOE

Table 3 Security objectives for the TOE

Security Objective	Description
O.AUDIT	The TOE shall be able to generate audit records for security-relevant events:

Security Objective	Description
	• user activity • user management The authorized use is able to query and filter security logs of TOE.
O.COMMUNICATION	The TOE must implement logical protection measures, which is including TLS/SSH, for network communication between the TOE and WebLMT or U2020 server, and securely manage AES and HASH cryptographic functionalities to support confidentiality and integrity for transmitting data.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network. TOE can authenticate users via physical interfaces, logical communication interfaces, and protocols, which can prevent unauthorized access. The TOE shall support user authentication, allowing the TOE to accept or reject the users based on the response of the AAA (Authentication, Authorization and Accounting) service of TOE. The TOE shall provide security management functions on user management and configuration management depending on different user roles.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The following security objectives, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 4 Security objectives for the operational environment

Security Objective	Description
OE.PHYSICAL	The TOE, CloudOS, U2020 server and hardware driver are located in a physically protected environment which is protected against unauthorized physical access. Only trusted users are allowed to access it. Communication between the TOE and the U2020 server shall be physically isolated by using an ethernet cable connecting the two endpoints.
OE.LIMITED_FUNCTIONALITY	The hardware, CloudOS and U2020 server, where the TOE is installed, only provides services that support TOE's running, operation, and management, while it only provides networking functionality as its function and does not provide functionality or services that could be deemed as general-purpose computing.
OE.TRUSTED_ADMIN	TOE users are trusted to follow and apply all guidance documentation in a trusted manner. TOE users are appropriately trained. TOE users shall ensure passwords/credentials are set with sufficient strength and without malicious intent when administering the device.
OE.ADMIN_CREDENTIALS_SECURE	The TOE user's credentials (private key) used to access the TOE are protected by any other platform which they reside and are encrypted by AES CBC 128bits algorithm.
OE.COMPONENTS_RUNNING	The TOE environments (U2020 server, CloudOS and hardware driver) shall work properly.
OE.RESIDUAL_INFORMATION	The TOE has no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is not in its operational environment.

Security Objective	Description
OE.NETWORK_ SEGREGATION	The TOE is isolated based on proper configurations, to prevent data outside of TOE to affect TOE.
OE.TIME	The CloudOS provides the reliable timestamps to the TOE.
OE.ENVIRONMENT_ACL	The TOE environment (virtual vSwitch) provides external access only to the TOE interfaces through ACL rules.

4.3 SECURITY OBJECTIVES RATIONALE

The tracing shows how the security objectives trace back to the threats, OSPs and assumptions as described in the security problem definition. The security objectives rationale also demonstrates that all the given threats, OSPs and assumption are addressed.

Table 5 Security objectives for the rationale

Objective	Threat/OSPs/Assumption	Rationale for security objectives
O.AUDIT	OSP.AUDIT	The security policy OSP.AUDIT is answered by the security objective for the TOE O.AUDIT which requires the TOE to generate audit records and properly handle audit records.
O.IDAUTH **O.COMMUNICATION**	T.UNTRUSTED_COMMUNICATION_CHANNELS	The threat T.UNTRUSTED_COMMUNICATION_CHANNELS is answered by the security objective for the TOE O.IDAUTH which requires all logical communication interfaces and protocols, which manage the TOE, are authenticated to prevent unauthorized access. O.COMMUNICATION requires that TOE manages secure connections to WebLMT or U2020 server to protect confidentiality and integrity for transmitting data.
O.IDAUTH **OE.TRUSTED_ADMIN** **OE.PHYSICAL** **OE.RESIDUAL_INFORMATION** **OE.ADMIN_CREDENTIALS_SECURE**	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	The threat T.UNAUTHORIZED_ADMINISTRATOR_ACCESS is answered by the following items: The security objective for the TOE O.IDAUTH which requires the TOE to implement an authentication mechanism for the users, and requires the TOE to implement an access control mechanism for the users in the management network. OE.TRUSTED_ADMIN requires that TOE users follow and apply all guidance documentation in a trusted manner.

Objective	Threat/OSPs/Assumption	Rationale for security objectives
		OE.PHYSICAL requires that TOE and TOE environment (U2020 server, CloudOS and hardware driver) are protected against unauthorized physical access. OE.RESIDUAL_INFORMATION requires that system user of TOE ensures that the sensitive residual data are controlled by access permission. OE.ADMIN_CREDENTIALS_SECURE requires that user's credential is stored on any other platform and encrypted by AES CBC 128bits algorithm.
O.IDAUTH **O.COMMUNICATION** **OE.NETWOR_SEGREGATION** **OE.RESIDUAL_INFORMATION**	T.WEAK_AUTHENTICATION_ENDPOINTS	The threat T.WEAK_AUTHENTICATION_ENDPOINTS is answered by the security objective for the TOE O.IDAUTH which requires the TOE to implement an authentication mechanism for the local users, and requires the TOE to implement an access control mechanism for the users in the management network. It is also answered by requiring communications security via TLS/SSH for network communication between entities in the management network and the TOE (O.COMMUNICATION), and requiring that TOE is isolated based on proper configurations, to prevent data outside of TOE affecting TOE (OE.NETWOR_SEGREGATION). It is also answered by requiring that the sensitive residual data on the device is forcibly deleted, or the access permission is controlled. (OE.RESIDUAL_INFORMATION)
O.COMMUNICATION	T.WEAK_CRYPTOGRAPHY	The threat T.WEAK_CRYPTOGRAPHY is answered by the security objective for the TOE O.COMMUNICATION which requires the TOE to encrypt authorized user identities and data and manages keys and protect confidentiality and integrity for transmitting data.

Objective	Threat/OSPs/Assumption	Rationale for security objectives
OE.PHYSICAL	A.PHYSICAL_PROTECTION	OE.PHYSICAL ensures that TOE and its environment are located in an authorized accessible place which is protected against unauthorized physical access.
OE.LIMITED_FUNCTIONALITY	A.LIMITED_FUNCTIONALITY	OE.LIMITED_FUNCTIONALITY ensures that TOE can only perform limited functionalities defined in Section 5, but not perform general-purpose computing.
OE.TRUSTED_ADMIN	A.TRUSTED_ADMINISTRATOR	OE.TRUSTED_ADMIN ensures that TOE users operate TOE as following guidance documentations in a trusted manner and are appropriately trained. And TOE users ensure passwords/credentials are set with sufficient strength and without malicious intent when administering the device.
OE.COMPONENTS_RUNNING	A.COMPONENTS_RUNNING	OE.COMPONENTS_RUNNING ensures that TOE environments (U2020 server, CloudOS and hardware driver) work properly.
OE.ADMIN_CREDENTIALS_SECURE	A.ADMIN_CREDENTIALS_SECURE	OE.ADMIN_CREDENTIALS_SECURE ensures that user's credentials, which are used to access TOE, are protected confidentiality by AES algorithm, on the platform which they reside.
OE.RESIDUAL_INFORMATION	A.RESIDUAL_INFORMATION	OE.RESIDUAL_INFORMATION ensures that all sensitive residual data on the device is forcibly deleted, or not accessible, once the device is discarded or removed from the TOE operation environment.
OE.NETWORK_SEGREGATION	A.NETWORK_SEGREGATION	OE.NETWORK_SEGREGATION ensures that TOE is isolated based on proper configuration, to prevent data outside of TOE to affect TOE.
OE.TIME	A.TIME	OE.TIME ensures that the CloudOS provides the reliable timestamps.
OE.ENVIRONMENT_ACL	A.ENVIRONMENT_ACL	OE.ENVIRONMENT_ACL ensures that the virtual vSwitch provides external access only to the TOE interfaces through ACL rules.

5 SECURITY REQUIREMENTS FOR THE TOE

This section provides functional and assurance requirements that satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1 CONVENTIONS

The following conventions are used for the completion of operations:

~~Strikethrough~~ indicates text removed as a refinement

(Underlined text in parentheses) indicates additional text provided as a refinement.

[Bold text] indicates the completion of an assignment.

[*Italicized and bold text*] indicates the completion of a selection.

Iteration/N indicates an element of the iteration, where N is the iteration number/character.

5.2 SECURITY FUNCTIONAL REQUIREMENTS

The functional security requirements for the TOE consist of the following components from Part 2 of the CC, summarized in the following table.

Table 6 Security Functional Requirements

	Functional Requirements
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FIA_UAU.4	Single-use authentication mechanisms
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SAE.1	Time-limited authorization
FTA_MCS.1/WebLMT	Basic limitation on multiple concurrent sessions
FTA_MCS.1/U2020	Basic limitation on multiple concurrent sessions
FTA_TSE.1	TOE session establishment
FTA_SSL.3	TSF-initiated termination

	Functional Requirements
FTP_TRP.1	Trusted path
FTP_ITC.1	Inter-TSF trusted channel

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit data generation

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

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

b) All auditable events for the **[*not specified*]** level of audit; and

c) [The following auditable events:

i. authentication management

1. login, logout

2. any failure of authentication

ii. user management

1. add, delete, modify

2. password change

iii. session management

1. failure of session establishment

2. session time-out management].

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, **[interface (if applicable), workstation IP (if applicable), User name (if applicable), and MML command name (if applicable), security severity level of the event].**

Application note:

- event ‘session time-out management’ is only applicable for HTTPs session.
- event ‘any failure of authentication’ is recorded only through SSH interface.
- event ‘failure of session establishment’ is only applicable for SSH session.
- event ‘Start-up and shutdown of the audit functions’ is occurred at the same time of TOE start-up, the audit log is recorded during TOE start-up.

5.2.1.2 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.

5.2.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **[users authorized per FDP_ACF.1]** with the capability to read **[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.

5.2.1.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **[filtering]** of audit data based on **[date and time of the event, security severity level of the event]**.

5.2.1.5 FAU_STG.1 Protected audit trail storage

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

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

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

FAU_STG.3.1 The TSF shall **[delete the oldest files]** if the audit trail exceeds **[8MB]**.

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[access control policy]** on **[**

Subject: user;

Objects: user data, audit logs, SSH configuration parameters, TLS configuration parameters, access control list;

Operation: add, modify, query, delete

]

Application note: user of manage-ug, system-ug, monitor-ug or visit-ug is only applicable to log in TOE through WebLMT, while user of ems-ug is only applicable to log in TOE through U2020. And it is only allowed username ‘emscomm’ to log in TOE through U2020.

5.2.2.2 FDP_ACF.1 Security attribute based access control

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

Subject:

- **user**

Subjects attributes: user role;

Objects: user data, audit logs, SSH configuration parameters, TLS configuration parameters, access control list]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**

a) A user with the security attribute "manage-ug" or "ems-ug" is allowed to perform commands (operations) that

query user data, audit logs, SSH configuration parameters, TLS configuration parameters, access control list,

add, modify and remove user data, SSH configuration parameters, TLS configuration parameters, access control list.

b) A user with the security attribute "system-ug" is allowed to perform commands (operations) that

query user data for the user's own only, TLS configuration parameters, access control list,

add, modify and remove access control list.

c) A user with the security attribute "monitor-ug" is allowed to perform commands (operations) that

query user data for the user's own only, TLS configuration parameters, access control list,

d) A user with the security attribute "visit-ug" is allowed to perform commands (operations) that query user data for the user's own only.

]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[None]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[None]**

Application note: user of manage-ug, system-ug, monitor-ug or visit-ug is only applicable to log in TOE through WebLMT, while user of ems-ug is only applicable to log in TOE through U2020. And it is only allowed username 'emscomm' to log in TOE through U2020.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 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.

5.2.3.2 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.

5.2.3.3 FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **[authentication mechanism for identifying management network access personnel]**.

5.2.3.4 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **[*3*]** unsuccessful authentication attempts occur related to **[user login within 5 minutes]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **[*met*]**, the TSF shall **[lockout the account for 5 minutes]**.

5.2.3.5 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[**

- **a) user ID**
- **b) user group**
- **c) password**
- **d) password expiration date for WebLMT user**
- **e) user account life]**

5.2.3.6 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet: **[A password is an 8-to-32-character string that contains letters, numerals and special characters. The letters are case sensitive. The password must adhere to the password policy, refer to Section 6.3]**.

Application note: During the password change procedure and during the login procedure, if the password inserted has more than 32 characters, it is truncated and only the first 32 characters are considered for the password.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_SMF.1 Specification of Management Functions

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

- **a) user management (addition, deletion, modification, querying)**
- **b) Modify TLS configuration of TLS version, cipher suite**
- **c) Modify SSH configuration of SSH algorithms, session management parameters**
- **d) Query configurations of TLS and SSH**
- **e) Query and modify access control list**

]

5.2.4.2 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: **[**

- **a) system-ug**
- **b) monitor-ug**

c) **manage-ug, ems-ug**

d) **visit-ug**

]

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.4.3 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **[*determine the behaviour of*]** the functions

- **[all functions defined in FMT_SMF.1.1]** to **[manage-ug, ems-ug]**
- **[Query user data for user's own only, TLS configuration parameters, access control list, and modify access control list]** to **[system-ug]**
- **[Query user data for user's own only, TLS configuration parameters, access control list]** to **[monitor-ug]**
- **[Query user data for user's own only]** to **[visit-ug]**

Application note: user of manage-ug, system-ug, monitor-ug or visit-ug is only applicable to log in TOE through WebLMT, while user of ems-ug is only applicable to log in TOE through U2020. And it is only allowed username 'emscomm' to log in TOE through U2020.

5.2.4.4 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[access control policy]** to restrict the ability to **[*query, modify*]** the security attributes **[listed in FDP_ACF.1]** to **[manage-ug, ems-ug]**.

Application note: the attributes User ID and Unsuccessful authentication attempt since last successful authentication attempt count cannot be modified.

5.2.4.5 FMT_MSA.3 Static attribute initialisation

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

FMT_MSA.3.2 The TSF shall allow the **[manage-ug, ems-ug]** to specify alternative initial values to override the default values when an object or information is created.

Application note: user of manage-ug, system-ug, monitor-ug or visit-ug is only applicable to log in TOE through WebLMT, while user of ems-ug is only applicable to log in TOE through U2020. And it is only allowed username 'emscomm' to log in TOE through U2020.

5.2.4.6 FMT_SAE.1 Time-limited authorisation

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for **[user account life and passwords]** to **[manage-ug, ems-ug].**

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to **[deny authentication]** after the expiration time for the indicated security attribute has passed.

Application note: user of manage-ug, system-ug, monitor-ug or visit-ug is only applicable to log in TOE through WebLMT, while user of ems-ug is only applicable to log in TOE through U2020. And it is only allowed username 'emscomm' to log in TOE through U2020.

5.2.5 TOE Access (FTA)

5.2.5.1 FTA_MCS.1/WebLMT Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user**.**

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [**3**] sessions per user.

Application note: for each user session, WebLMT will establish 2 HTTPs sessions to connect to TOE.

5.2.5.2 FTA_MCS.1/U2020 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user**.**

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [**1**] sessions per user.

Application note: for each user session, U2020 will establish 2 SSH sessions to connect to TOE.

5.2.5.3 FTA_TSE.1 TOE session establishment

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

a) IP address

b) Blacklist]

5.2.5.4 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **[10 minutes of user inactivity]**.

Application note: this SFR is only application on HTTPs session.

5.2.6 Trusted Path/Channels (FTP)

5.2.6.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **[*remote*]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[*modification, disclosure*].**

FTP_TRP.1.2 The TSF shall permit **[*remote users*]** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **[*connecting with the WebLMT through a TLS channel to manage the TOE*]**.

5.2.6.2 FTP_ITC Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [***U2020 server***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**connecting with U2020 server through SSH channel to manage the TOE**].

5.3 SECURITY REQUIREMENTS DEPENDENCY RATIONALE

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 modelled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Table 7 Dependencies between TOE Security Functional Requirements

Security Functional Requirement	**Dependencies**	**Resolution**
FAU_GEN.1	FPT_STM.1	It is met by OE.TIME that the CloudOS provides reliable timestamps to TOE.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FIA_UID.2	None	N.A.
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.4	None	N.A.
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	N.A.
FIA_SOS.1	None	N.A.
FMT_SMF.1	None	N.A.
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SAE.1	FMT_SMR.1 FPT_STM.1	FMT_SMR.1 FPT_STM.1 is met by OE.TIME that the CloudOS provides reliable timestamps to TOE.
FTA_MCS.1/WebLMT	FIA_UID.1	FIA_UID.2
FTA_MCS.1/U2020	FIA_UID.1	FIA_UID.2

Security Functional Requirement	Dependencies	Resolution
FTA_TSE.1	None	N.A.
FTA_SSL.3	None	N.A.
FTP_TRP.1	None	N.A.
FTP_ITC.1	None	N.A.

5.4 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

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

The security objectives are covered by the security functional requirements, shown as Table 9.

Table 8 Coverage for the Security Objectives

	O.AUDIT	O.IDAUTH	O.COMMUNICATION
FAU_GEN.1	X		
FAU_GEN.2	X		
FAU_SAR.1	X		
FAU_SAR.3	X		
FAU_STG.1	X		
FAU_STG.3	X		
FDP_ACC.1		X	
FDP_ACF.1		X	
FIA_UID.2		X	
FIA_UAU.2		X	
FIA_UAU.4		X	
FIA_AFL.1		X	
FIA_ATD.1		X	
FIA_SOS.1		X	
FMT_SMF.1		X	X
FMT_SMR.1		X	
FMT_MOF.1		X	
FMT_MSA.1		X	
FMT_MSA.3		X	
FMT_SAE.1		X	
FTA_MCS.1/WebLMT		X	
FTA_MCS.1/U2020		X	
FTA_TSE.1		X	
FTA_SSL.3		X	
FTP_TRP.1			X

	O.AUDIT	O.IDAUTH	O.COMMUNICATION
FTP_ITC.1			X

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

Table 9 Rationale for the Security Requirements

Rationale	Security objectives
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 identification mechanism. Functionality is provisioned to read these records (FAU_SAR.1, FAU_SAR.3). The protection of the stored audit records is implemented in FAU_STG.1. Functionality to prevent audit data loss is provided by FAU_STG.3.	O.AUDIT
User authentication is implemented by FIA_UAU.2 and FIA_UAU.4. Individual user identification is implemented in FIA_UID.2. The necessary user attributes are spelled out in FIA_ATD.1. The authentication mechanism supports authentication failure handling (FIA_AFL.1), and a password policy (FIA_SOS.1), restrictions as to the validity of accounts for logon (FTA_TSE.1). Security management functionality, which includes user management and configuration management, is provided in FMT_SMF.1. Security roles definition is FMT_SMR.1. Security functions behaviour management is FMT_MOF.1. Security attribute management is FMT_MSA.1 and FMT_MSA.3. And time-limited authorization is FMT_SAE.1. TLS session termination function is provided in FTA_SSL.3. TLS/SSH session number limit is provided in FTA_MCS.1/WebLMT and FTA_MCS.1/U2020. Functionality to deny TLS/SSH session is provided in FTA_TSE.1. The access control policy is implemented by FDP_ACC.1 and FDP_ACF.1.	O.IDAUTH
Management functionality to enable these mechanisms is provided in FMT_SMF.1. The communication path protection between TOE and WebLMT is provided in FTP_TRP.1. The communication path protection between TOE and U2020 server is provided in FTP_ITC.1.	O.COMMUNICATION

5.5 SECURITY ASSURANCE REQUIREMENTS

The security assurance requirements for the TOE are the Evaluation Assurance Level 4 components as specified in [CC] Part 3, augmented with ALC_FLR.1. No operations are applied to the assurance components.

Table 10 Security Assurance Requirements

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level
Development	ADV_ARC	1
	ADV_FSP	4
	ADV_IMP	1
	ADV_TDS	3
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	1
	ALC_LCD	1
	ALC_TAT	1
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	3

5.6 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.

6 TOE SUMMARY SPECIFICATION

6.1 AUDITING

Removing the logs is always forbidden (FAU_STG.1)

There exist two kinds of audit files, the operation log and the security log.

1) Operation logs: Records operations that users perform on the system using configuration tools and operations that the system automatically performs.

2) Security logs: process, and error information of system account management security, protocol security, attack defence security, and status security in real time.

Each type of log file defines 1000 as the maximum number of audit records supported to be stored. If the audit record number of the log file exceeds the maximum number threshold, the latest audit record will be dropped. If the storage capacity reached the threshold (8MB), the latest log will overwrite the earliest log. (FAU_STG.3)

Log files are prevented to be modified or deleted by any user who can access to the TOE, that TOE doesn't provide an interface to modify or delete log files. (FAU_STG.1)

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include identification and authentication related events, and user logging-in or logging-out events and communication session events. Each of the events specified in the audit record is in enough detail to identify the user for which the event is associated (e.g., user identity, MAC address, IP address), when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred.

The audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record contains a lot of information, such as the type of event that occurred. As noted above, the information includes at least all of the required information. Additional information can be configured and included if desired. (FAU_GEN.1, FAU_GEN.2)

Users with the appropriate rights can review the audit records available in the database. The TOE offers search functionality based on time range and security severity level. (FAU_SAR.1, FAU_SAR.3)

6.2 COMMUNICATION SECURITY

The TOE provides a trusted communication channel between the TOE and WebLMT/U2020.

When using maintenance terminals to perform OM operations for the TOE, carriers can use HTTPs/SSH to ensure the security of data transmission and maintenance interfaces on the TOE.

The TOE generates key pair or key for each session for security communication, which prevents reuse of authentication data. (FIA_UAU.4)

6.2.1 HTTPs

HTTPs provides the following security services for the communication between TOE and WebLMT:

- Connection privacy

Connection privacy means that data is encrypted before transmission to prevent data from being hacked by malicious users. HTTPs enables confidentiality by using encryption algorithms. Common encryption algorithms are AES128/256 GCM. AES keys are derived from shared secret, which is calculated from key agreement between TOE and WebLMT. DH-scheme key pair or ECC-scheme key pair for key agreement is generated by TOE and WebLMT during HTTPs session establishment.

- Data integrity

Data integrity means that any modification to data during transmission can be detected. HTTPs via TLS establishes a secure channel between the client and the server and uses message digest algorithms (SHA256) to ensure data integrity so that all the data processed by HTTPs can reach the destination without being modified.

The TOE supports HTTP via TLS, which is versions TLS1.2.

TLS protocol supports cipher suite:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

(FTP_TRP.1)

6.2.2 SSH

SSH provides the following security services for the communication between TOE and U2020 server:

TOE can provide security services SSH v2.0 to protect the integrity and privacy of transmitting data between TOE and U2020 server, by encryption and hashing of the data.

TOE derive AES keys from shared secret, which is calculated from key agreement between TOE and U2020 server. DH-scheme key pair or ECDH-scheme key pair for key agreement is generated by TOE and WebLMT during HTTPs session establishment.

SSH protocol supports cipher suite:

Host public key algorithm: ecdsa-sha2-nistp521

Encryption algorithm:

- AES_256_CTR
- AES_128_CTR

HMAC algorithm:

- hmac-sha2-256

key exchange algorithm:

- ecdh-sha2-nistp521

(FTP_ITC.1)

6.3 AUTHENTICATION

The authorized users are able to configure a system-wide password policy that is then enforced by the TOE. Username supports 1-32 characters, case-insensitive characters. The password is a string of 8 to 32 characters. 1: The password is case-sensitive. 2: The password must contain digits, uppercase letters, lowercase letters, and special characters, except for commas (,), semicolons (;), equal signs (=), double quotation marks ("), single quotation marks, question marks (?), and spaces. 3: The password must not contain the username or its reverse form. 4: The password must be different from 10 latest historical passwords. Entering a password which is same as an existing password, is not allowed, either. (FIA_SOS.1)

During user creation, the user group, which is one of user attributes, is set as the user role to category the user having the corresponding security functions access, refer to Table 11 for matrix of user group and user role. (FMT_SMR.1, FIA_ATD.1)

Table 11 Matrix table for user group and user role

user group	user role

system-ug	system user
manage-ug ems-ug	manage user
monitor-ug	monitor user
visit-ug	visit user

A user group defines a set of rights for different user type. A command group is a set of commands. A user group can be authorized rights via command groups, a user group may include more than one command groups. Commands are classified into command groups, and then the command groups are assigned to users with different authorities, realizing authority management. (FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3)

Table 12 User level and authorized functions

User Role	Rights
manage-ug, ems-ug	A user of this role is allowed to perform commands which include: • Query security and operation logs, • Create SSL policy, • Delete SSL Policy, • Modify SSL Policy, • List SSL Policy, • Create SSL cipher suite, • Delete SSL cipher suite, • Modify SSL cipher suite, • List SSL cipher suite, • Set SSH client encryption algorithm, • List SSH client encryption algorithm, • Set SSH client HMAC algorithm, • List SSH client HMAC algorithm, • Set SSH client key exchange algorithm, • List SSH client key exchange algorithm, • Create ACL rule group, • Delete ACL rule group, • Modify ACL rule group, • List ACL rule group, • Create basic ACL rule, • Delete basic ACL rule, • Modify basic ACL rule, • List basic ACL rule, • Add local user, • Delete local user, • Modify local user, • List local user, • Set SSH server parameters, • List SSH server parameters, • Set WebLMT server parameters, • List WebLMT server parameters.

User Role	Rights
system-ug	A user of this role is allowed to perform commands which include: • List SSL Policy, • List SSL cipher suite, • Create ACL rule group, • Delete ACL rule group, • Modify ACL rule group, • List ACL rule group, • Create basic ACL rule, • Delete basic ACL rule, • Modify basic ACL rule, • List basic ACL rule, • List local user (only list user's own user data), • List WebLMT server parameters.
monitor-ug	A user of this role is allowed to perform commands which include: • List SSL Policy, • List SSL cipher suite, • List ACL rule group, • List basic ACL rule, • List local user (only list user's own user data), • List WebLMT server parameters.
visit-ug	A user of this role is allowed to perform commands which include: • List local user. (only list user's own user data)

Commands are classified into command groups and command groups are assigned to users with different rights. One command belongs to only one specific command group. The system provides eight predefined command groups. The commands contained in these command groups cannot be modified. This means that a command group to which a command belongs cannot be changed, and rights can be assigned only by specifying command groups. (FMT_MOF.1)

The TOE can identify local users in the management network by a unique username and enforces their authentication before granting them access to the TSF management interfaces. Error message "Incorrect username or password or log in restricted" will be returned when the user fails to provide a correct username or password. The password of each user account has expiration date, by default, password expiration date is set as 90 days after user account creation. During login, if the password expired, TOE shall force user to change password by providing current password and new password. The user account life is permanently valid by default. The user account life of users could be configurable as 1-365 days or 65535 days during the user account creation or user account re-activation. If the user doesn't login within user account life, the user account is locked, and error message "Incorrect username or password or log in restricted" is returned during login. (FIA_UID.2, FIA_UAU.2, FIA_ATD.1)

The TOE supports to lockout the user for 5 minutes once 3 attempts due to authentication failure for this user within 5 minutes. This function is achieved by providing counts on authentication failure.

The TOE also offers the enforcement of permanent or timer-based account lockouts: a user in manage-ug or ems-ug can specify after how many consecutively failed authentications attempts an account will be

permanently or temporarily locked, and whether the counter for failed attempts will be reset automatically after 5 minutes.

When a session is inactive for a configured period of time, the TOE will lock this session and the user needs to re-enter his password to unlock the session. (FIA_AFL.1, FMT_SAE.1)

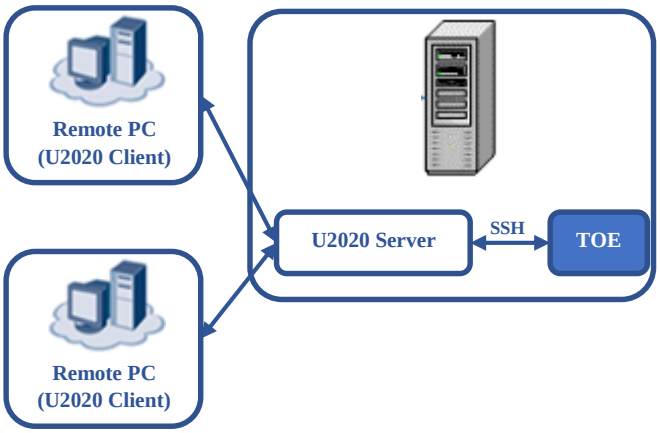
6.4 ACCESS CONTROL

The access control feature enables carriers to manage user authorities to ensure that only authorized users are allowed to operate the TOE within the authorization range, such as adding, modifying, or deleting users, logging in or logging out users, and assigning rights to users.

TOE can enforce the account locking function for the user access control.

The TOE supports a maximum of 6 concurrent sessions per user for the WebLMT login. The TOE supports only 1 concurrent session per user for the U2020 login TOE. (FTA_MCS.1/WebLMT, FTA_MCS.1/U2020)

Note: U2020 Server supports multiple concurrent session per user for U2020 client to login U2020 server. However, this concurrent session management is out of this evaluation scope. (see the chart as below)



When a user is not active, the account can be locked to prevent unauthorized access to the system.

If a user in manage-ug or ems-ug has specified values for these parameters for a specific user, the TOE will deny authentication of the user if the number of “account valid days (365 days by default)” configured for the user has been exceeded, if the password has not been changed within the timeframe specified in the “password valid days” configuration for the user, or 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. (FTA_SSL.3)

6.4.1 ACL

The TOE supports IP-based Access Control List (ACL) to prevent internal traffic overload and service interruption.

The TOE also uses the ACL to identify flows and prevent the CPU and related services from being attacked.

1) Support enabling ACLs by associating ACLs to whitelist, blacklist, user-defined-flow. This function is achieved by interpreting ACL configurations then storing interpreted value in memory.

2) Support screening, filtering traffic destined to CPU. This function is achieved by downloading ACL configurations into hardware.

The TOE can use the ACL to deny the network's data packet based on some criteria defined in the ACL such as destination IP address.

The TOE can flexibly set the ACL rules for the user-defined flows to prevent unidentified attacks in the network. In addition, the characteristics of the attack data flows can be specified and rules for filtering the data flows of these characteristics can be set.

The TOE can use the APN based on ACL to deny the user's data packet based on some criteria defined in the ACL such as destination IP address.

The access sources can be specified to restrict the scope of access devices. For example, an access control list (ACL) can be defined to filter access users based on their IP addresses or specify the source interfaces through which users are allowed to log in.

(FIA_AFL.1, FTA_TSE.1, FMT_SMF.1)

6.5 SECURITY MANAGEMENT

The TOE offers management functionality for its security functions, where appropriate. This is partially already addressed in more detail in the previous sections of the TSS, but includes:

1) User management (deletion, modification and addition**)**, including username, password, and User Group memberships, including the association of users and corresponding privileged functionalities, etc.
2) TLS configuration, authentication (certificate verification) and encryption.
3) SSH configuration, authentication (password and public key) and encryption, the duration of session time-out, access control, 3 attempts due to authentication failure within 1 minute.
4) Query TLS and SSH configuration of authentication and encryption.

Above functions are achieved by providing interpreting input commands and storing result of interpreting in memory. Some results like routes generated, ACLs will be downloaded into hardware to assist forwarding and other TSF functions.

(FMT_SMF.1)

7 ACRONYMS AND ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
ACL	access control list
AES	advance encryption standard
AES-GCM	AES Galois/Counter Mode
APN	Access point name
BSS	Business Support Systems
CA	Certificate authority
CGW	charging gateway
E-UTRAN	evolved UMTS terrestrial radio access network
ECC	Elliptic-curve cryptography
GGSN	gateway GPRS support node
GPRS	general packet radio service
GSM	global system for mobile communications
HTTPs	Hypertext Transfer Protocol Secure
IPSec	Internet Protocol Security
LMT	local maintenance terminal
LTE	long term evolution
MANO	Management and Orchestration
MML	man-machine language
MS	Mobile Station
NE	network element
NFV	Network functions virtualization
NFVI	network functions virtualization infrastructure
NSA	Non-Standalone
O&M	operation and maintenance
PDN GW/P-GW	PDN gateway
S-GW	serving gateway
SGSN	serving GPRS support node supporting Rel-8 3GPP
SCP	service control point
SSH	Secure Shell
TLS	transport layer security
UDG	unified distributed gateway
UG	User group
UE	User equipment

UMTS	universal mobile telecommunications system
UNC	unified network controller
UTRAN	UMTS terrestrial radio access network
VNF	virtualized network function
VNFC	virtualized network function component
VPN	virtual private network
VRF	virtual routing and forwarding
WebLMT	web local maintenance terminal