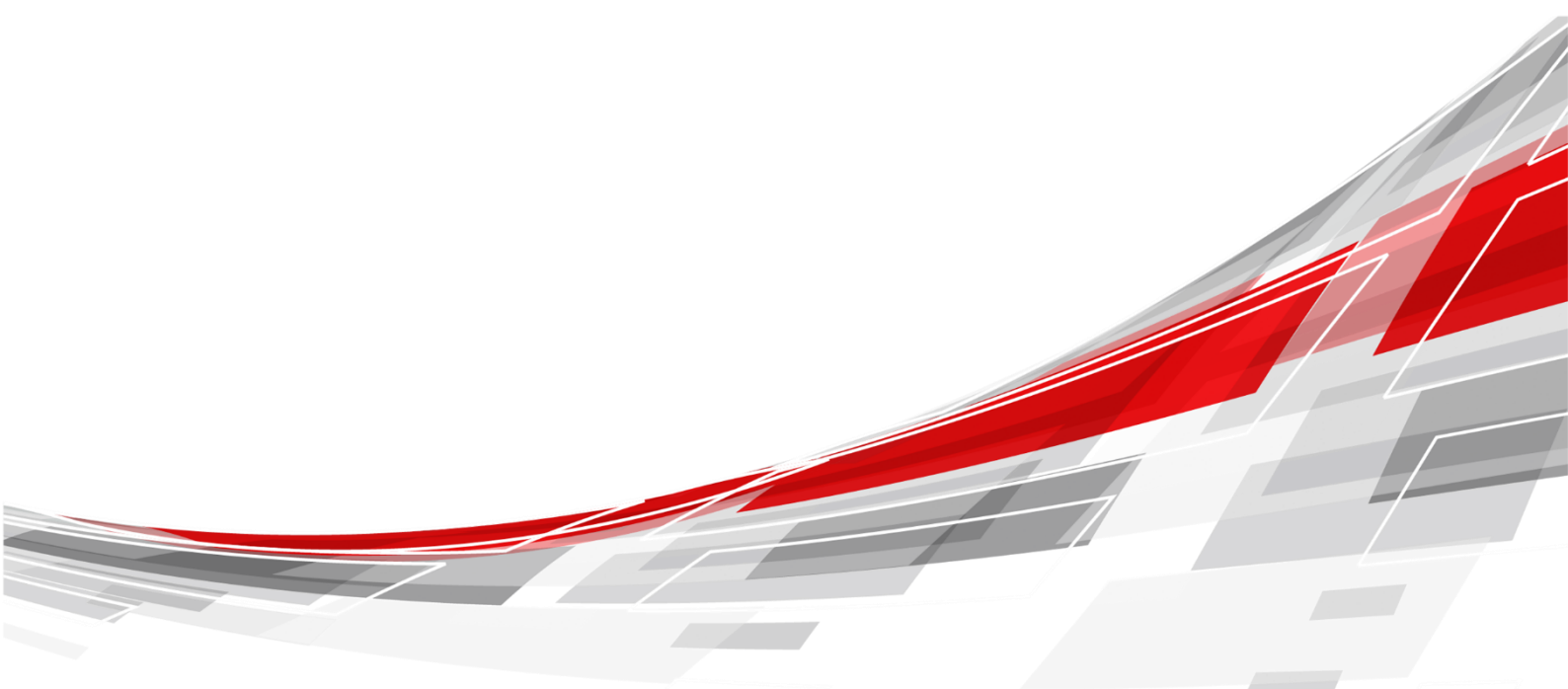


xFusion FusionDirector 1.7.1.SPC3 Security Target

Issue	V1.11
Date	2023-07-10



Copyrights © xFusion Digital Technologies Co., Ltd. 2022. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of xFusion Digital Technologies Co., Ltd.

Trademarks and Permissions

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

In this document, "xFusion" is used to refer to "xFusion Digital Technologies Co., Ltd." for concise description and easy understanding, which does not mean that "xFusion" may have any other meaning. Any "xFusion" mentioned or described hereof may not be understood as any meaning other than "xFusion Digital Technologies Co., Ltd.", and xFusion Digital Technology Co., Ltd. shall not bear any liability resulting from the use of "xFusion".

The purchased products, services and features are stipulated by the contract made between xFusion and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

xFusion Digital Technologies Co., Ltd.

Address: 9th Floor, Building 1, Zensun Boya Square, Longzihu Wisdom Island
Zhengdong New District 450046
Zhengzhou, Henan Province
People's Republic of China

Website: <https://www.xfusion.com>






About This Document

Purpose

This document provides description about ST (Security Target)

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
 NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Date	Revision Version	Change Description	Author
2022-02-15	1.0	The initial draft was complete.	Meng Xinping
2022-05-25	1.1	Updated according to the comments from Paliwal Himanshu	Meng Xinping
2022-07-22	1.2	Updated according to the comments from Marc Gómez Ciurana	Meng Xinping
2022-08-05	1.3	Updated according to the comments from Marc Gómez Ciurana	Meng Xinping
2022-08-11	1.4	Updated according to the comments from Marc Gómez Ciurana	Meng Xinping
2022-08-16	1.5	Updated according to the comments from Marc Gómez Ciurana	Meng Xinping
2022-10-25	1.6	Updated according to the comments from Marc Gómez Ciurana	Meng Xinping
2022-11-15	1.7	Updated according to the comments from Marc Gómez Ciurana	Meng Xinping
2022-12-25	1.8	Updated according to the comments from Marc Gómez Ciurana	Meng Xinping
2022-12-30	1.9	Updated according to the comments from Marc Gómez Ciurana	Meng Xinping
2023-02-03	1.10	Updated according to the comments from Marc Gómez Ciurana	Meng Xinping
2023-07-10	1.11	Updated according to the comments from Marc Gómez Ciurana	Meng Xinping

Contents

About This Document	ii
1 Introduction	1
1.1 Security Target Reference.....	1
1.2 TOE Reference.....	1
1.3 TOE Overview.....	1
1.3.1 General Product Overview.....	1
1.3.2 Non-TOE Hardware/Software/Firmware Required by the TOE.....	2
1.4 TOE Description.....	3
1.4.1 Architectural Overview of FusionDirector.....	3
1.4.1.1 Software Architecture of FusionDirector.....	3
1.4.2 Scope of Evaluation.....	4
1.4.2.1 Physical Scope.....	4
1.4.2.2 Logical Scope.....	4
1.4.3 Summary of Security Features.....	7
1.4.3.1 Authentication.....	7
1.4.3.2 Authorization.....	7
1.4.3.3 Access Control.....	9
1.4.3.4 Auditing.....	9
1.4.3.5 Communication Security.....	10
1.4.3.6 Cryptographic Functions.....	10
1.4.3.7 Digital Signature for Software Integrity Protection.....	10
2 CC Conformance Claim	12
3 TOE Security Problem Definition	13
3.1 Asset.....	13
3.2 Threats.....	13
3.3 Assumptions.....	17
4 Security Objectives	19
4.1 Objectives for the TOE.....	19
4.2 Objectives for the Operational Environment.....	20
4.3 Security Objectives Rationale.....	21
4.3.1 Coverage.....	21

4.3.2 Sufficiency	22
4.4 TSF and Non-TSF Data	24
5 Security Requirements	25
5.1 Conventions	25
5.2 Definition of Security Policies	25
5.2.1 Access Control Policy	25
5.3 TOE Security Functional Requirements	26
5.3.1 Security Audit (FAU)	26
5.3.1.1 FAU_GEN.1 Audit Data Generation	26
5.3.1.2 FAU_GEN.2 User Identity Association	27
5.3.1.3 FAU_SAR.1 Audit Review	27
5.3.1.4 FAU_STG.1 Protected Audit Trail Storage	27
5.3.1.5 FAU_STG.3 Action in Case of Possible Audit Data Loss	27
5.3.2 Cryptographic Support (FCS)	28
5.3.2.1 FCS_COP.1/AES Cryptographic Operation	28
5.3.2.2 FCS_COP.1/RSA Cryptographic Operation	28
5.3.2.3 FCS_COP.1/HMAC-SHA1 Cryptographic Operation	29
5.3.2.4 FCS_COP.1/HMAC-SHA2 Cryptographic Operation	29
5.3.2.5 FCS_COP.1/SHA256 Cryptographic Operation	29
5.3.2.6 FCS_COP.1/SHA384 Cryptographic Operation	29
5.3.2.7 FCS_COP.1/PBKDF2 Cryptographic Operation	29
5.3.2.8 FCS_CKM.1/DH Cryptographic Key Generation	29
5.3.2.9 FCS_CKM.1/RSA Cryptographic Key Generation	30
5.3.2.10 FCS_CKM.4/RSA Cryptographic Key Destruction	30
5.3.3 User Data Protection (FDP)	30
5.3.3.1 FDP_ACC.1 Subset Access Control	30
5.3.3.2 FDP_ACF.1 Security Attribute Based Access Control	31
5.3.3.3 FDP_DAU.1 Basic Data Authentication	32
5.3.3.4 FDP_DAU.2 Data Authentication with Identity of Guarantor	32
5.3.3.5 FDP_IFC.1 Subset Information Flow Control	32
5.3.3.6 FDP_IFF.1 Simple Security Attributes	32
5.3.3.7 FDP_RIP.1 Subset Residual Information Protection	33
5.3.4 Identification and Authentication (FIA)	33
5.3.4.1 FIA_AFL.1 Authentication Failure Handling	33
5.3.4.2 FIA_ATD.1 User attribute definition	34
5.3.4.3 FIA_UAU.2 User authentication before any action	34
5.3.4.4 FIA_UID.2 User identification before any action	34
5.3.5 Security Management (FMT)	34
5.3.5.1 FMT_MOF.1 Management of Security Functions Behavior	34
5.3.5.2 FMT_MSA.1/ACFATD Management of Security Attributes	34
5.3.5.3 FMT_MSA.1/IFF Management of Security Attributes	35

5.3.5.4 FMT_MSA.3/ ACFATD Static Attribute Initialization	35
5.3.5.5 FMT_MSA.3/ IFF Static attribute initialization	35
5.3.5.6 FMT_SMF.1 Specification of Management Functions	35
5.3.5.7 FMT_SMR.1 Security roles	35
5.3.6 Protection of the TSF (FPT)	37
5.3.6.1 FPT_STM.1 Reliable time stamps	37
5.3.7 TOE access (FTA)	37
5.3.7.1 FTA_SSL.3 TSF-initiated termination	37
5.3.7.2 FTA_TSE.1 TOE session establishment	37
5.3.8 Trusted Path/Channels (FTP)	37
5.3.8.1 FTP_TRP.1 Trusted path	37
5.4 Security Functional Requirements Rationale	38
5.4.1 Coverage	38
5.4.2 Sufficiency	40
5.4.3 Security Requirements Dependency Rationale	43
5.4.4 Justification for Unsupported Dependencies	46
5.5 Security Assurance Requirements	46
5.6 Security Assurance Requirements Rationale	46
6 TOE Summary Specification	47
6.1 Authentication	47
6.2 Authorization	47
6.3 Auditing	49
6.4 Communication Security	50
6.5 Access Control	51
6.6 Security Management	51
6.7 Cryptographic Functions	53
6.8 Software Integrity Protection (Digital Signature)	54
7 Abbreviations, Terminology and References	55
7.1 Abbreviations	55
7.2 Terminology	56
7.3 References	57

List of Tables

Table 1: Default User roles and authority.....	8
Table 2: Mapping Objectives to Threats	22
Table 3: Mapping Objectives for the Environment to Threats, Assumptions	22
Table 4: Sufficiency analysis for threats.....	23
Table 5: Sufficiency analysis for assumptions	24
Table 6: Default User roles and authority.....	36
Table 7: Mapping SFRs to objectives.....	40
Table 8: SFR sufficiency analysis	42
Table 9: Dependencies between TOE Security Functional Requirements	46

List of Figures

Figure 1: Position of FusionDirector.	2
Figure 2: FusionDirector Software Architectural.	4
Figure 3: TOE logical scope.....	5
Figure 4: TOE Security functions.....	6

1 Introduction

This Security Target is for the CC evaluation of the xFusion FusionDirector 1.7.1.SPC3; the TOE consists of all of FusionDirector 1.7.1.SPC3 software except the underlying Guest OS.

1.1 Security Target Reference

Name: CC xFusion FusionDirector 1.7.1.SPC3 Security Target

Version: V1.11

Publication Date: 2023-07-10

Author: xFusion Digital Technologies Co., Ltd.

1.2 TOE Reference

Name: xFusion FusionDirector 1.7.1.SPC3

Version: 1.7.1.SPC3

Developer: xFusion Digital Technologies Co., Ltd.

The TOE is a software TOE consisting of all FusionDirector 1.7.1.SPC3 software except the underlying Guest OS as described in the following chapters. The main purpose of the TOE is Server management, including server query, status monitoring, configuration, firmware upgrade and OS deployment functions, etc. For details refer to chap. 1.4.2 .

1.3 TOE Overview

1.3.1 General Product Overview

xFusion FusionDirector enables unified server hardware O&M. Public cloud and enterprise customers can use FusionDirector to perform simple and efficient operation and maintenance (O&M) for xFusion servers in each phase of the life cycle to obtain ultimate experience.

FusionDirector implements visualized management and fault diagnosis for servers, and provides lifecycle management capabilities such as device management, device configuration, firmware upgrade, device monitoring, and OS deployment for xFusion servers, helping O&M personnel improve O&M efficiency and reduce O&M costs.

FusionDirector can be widely deployed in xFusion public cloud, private cloud, data center, carrier, and enterprise customers. It can be deployed in multiple scenarios such as Public Cloud, Private Cloud, NFVI and Traditional Data Center as shows in the following figure.

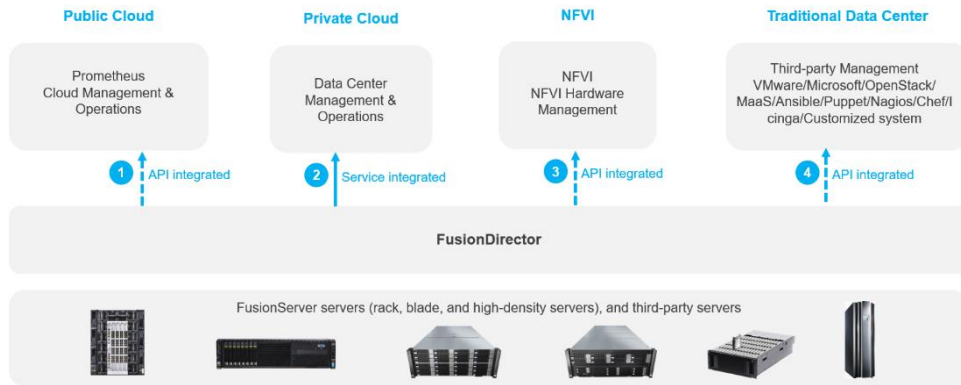


Figure 1: Position of FusionDirector.

1.3.2 Non-TOE Hardware/Software/Firmware Required by the TOE

The TOE is a server management software, it mainly implements server status monitoring, configuration, firmware upgrade, OS deployment functions. The TOE can run on virtual machine like KVM, VMware, Windows Hyper-V. The TOE can also operate on hardware server like 1288H V5 or 2288H V5. Specific installation environment requirements can refer to the installation guide.

1. The TOE is installed on the virtual machine. User needs to prepare virtual machines in advance according to the installation and deployment guidance. The network and operation security for the Host OS of the virtual machine and the hardware operating environment in which it is located should be ensured. The Host OS of virtual machine and the underlying Guest OS like Euler OS V2R10 are not in the scope of the TOE, but they are mandatory for the TOE.
2. The TOE is installed on the Hardware server, which is prepared by user. User should ensure the security of hardware networking and operation environment. The TOE installation hardware server is not in the scope of the TOE.
3. The supporting documents for internal usage are listed as below. The Installation Guide and Operation Guide will be modified only when there are new features, deleted features, or modified features in the software. If there are only bug fixes or small issues, these two documents will not be modified, and the document versions will remain unchanged.

Type	Delivery Item	Version
Software signature guidance	OpenPGP Signature Verification Guide.pdf	01
Product guidance	FusionDirector 1.7.1.SPC2 Installation Guide 01.pdf	01
	FusionDirector 1.7.1.SPC2 Operation Guide 01.pdf	01

1.4 TOE Description

This chapter provides an architectural overview of the FusionDirector including a detailed description of the software architecture, the definition of the TOE subject to evaluation and a summary of security functions provided by the TOE.

1.4.1 Architectural Overview of FusionDirector

xFusion FusionDirector is a software product, not applicable to hardware architecture, this section will introduce the xFusion FusionDirector software architecture.

xFusion FusionDirector software uses a micro service architecture with the following advantages:

- Low coupling. The coupling between micro-services is very small and can only communicate using Restful API or Message Queue (MQ).
- Good isolation, micro-services run in the Docker container. The communication between micro-services uses the Docker container network, which is isolated from the host network.
- Supporting scale out, supporting single-node, double-node or cluster (three-node or more) mode operation.
- Flexible deployment mode, supporting bare machine deployment and virtual machine deployment.

1.4.1.1 Software Architecture of FusionDirector

In terms of the software, the TOE's software architecture consists of one logical plane to support centralized management mechanism.

- Management plane

FusionDirector belongs to server management software, it mainly implements server status monitoring, configuration, firmware upgrade, OS deployment functions.

FusionDirector uses micro-service architecture, provides Restful API to the outside world, and uses reverse proxy to listen for external requests. All external messages are forwarded to API gateway by reverse proxy. API gateway realizes authentication and authorization of external messages through interaction with Identity and Access Management (IAM) micro-service. After authentication and authorization, the message is forwarded to the target micro-service for processing.

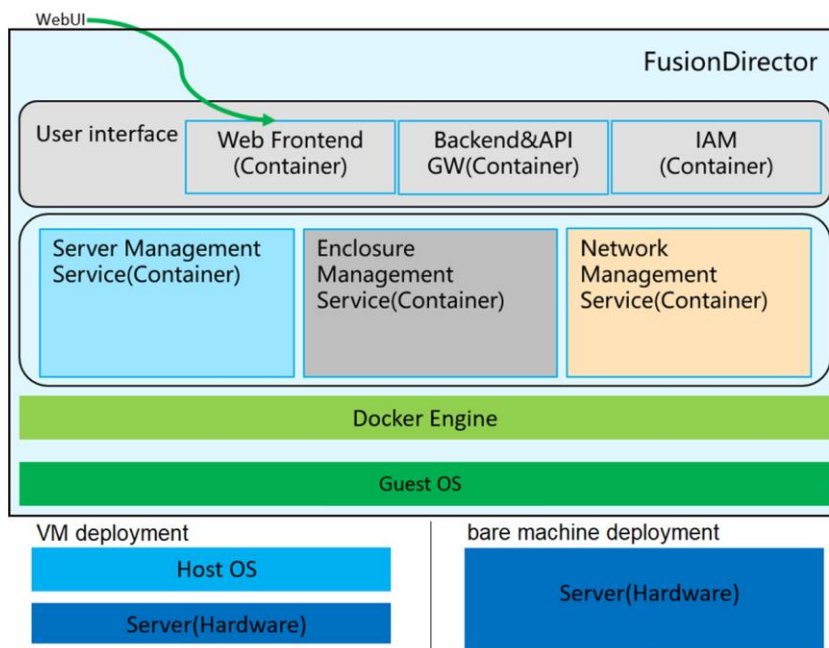


Figure 2: FusionDirector Software Architectural.

1.4.2 Scope of Evaluation

This section will define the scope of the part of the xFusion FusionDirector 1.7.1.SPC3 comprising the TOE to be evaluated.

1.4.2.1 Physical Scope

The TOE is software consisting of all FusionDirector 1.7.1.SPC3 software except the underlying Guest OS. This will be discussed in more detail in the next chapter. The evaluated configuration of the TOE is listed as below.

Type	Delivery Item	Version
Software	FusionDirector_1.7.1.SPC3_ENT_x86-64.qcow2	1.7.1.SPC3
Software signature file	FusionDirector_1.7.1.SPC3_ENT_x86-64.qcow2.p7s	1.7.1.SPC3
Product guidance	xFusion FusionDirector 1.7.1.SPC3 - AGD_OPE.docx	V1.10
	xFusion FusionDirector 1.7.1.SPC3 - AGD_PRE.docx	V1.6

1.4.2.2 Logical Scope

The logical boundary is represented by the elements that are displayed with a red frame within the rectangle in the figure below. The TOE consists of FusionDirector software except the underlying Guest OS(see red box in Figure 3).

The TOE provides several security functions which are described in more detail in chap. 1.4.3 .

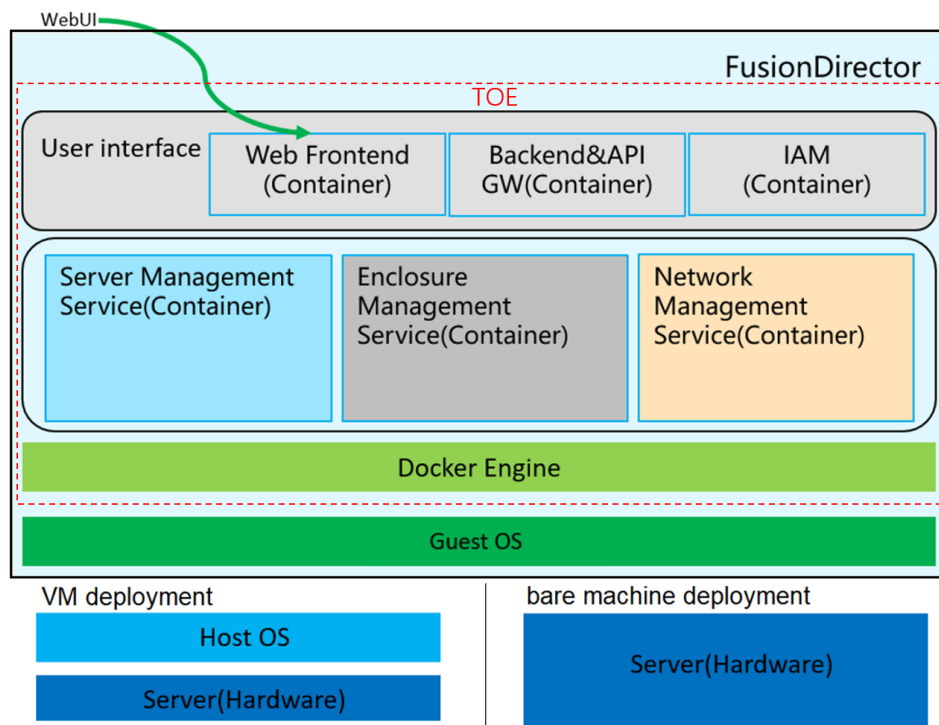


Figure 3: TOE logical scope.

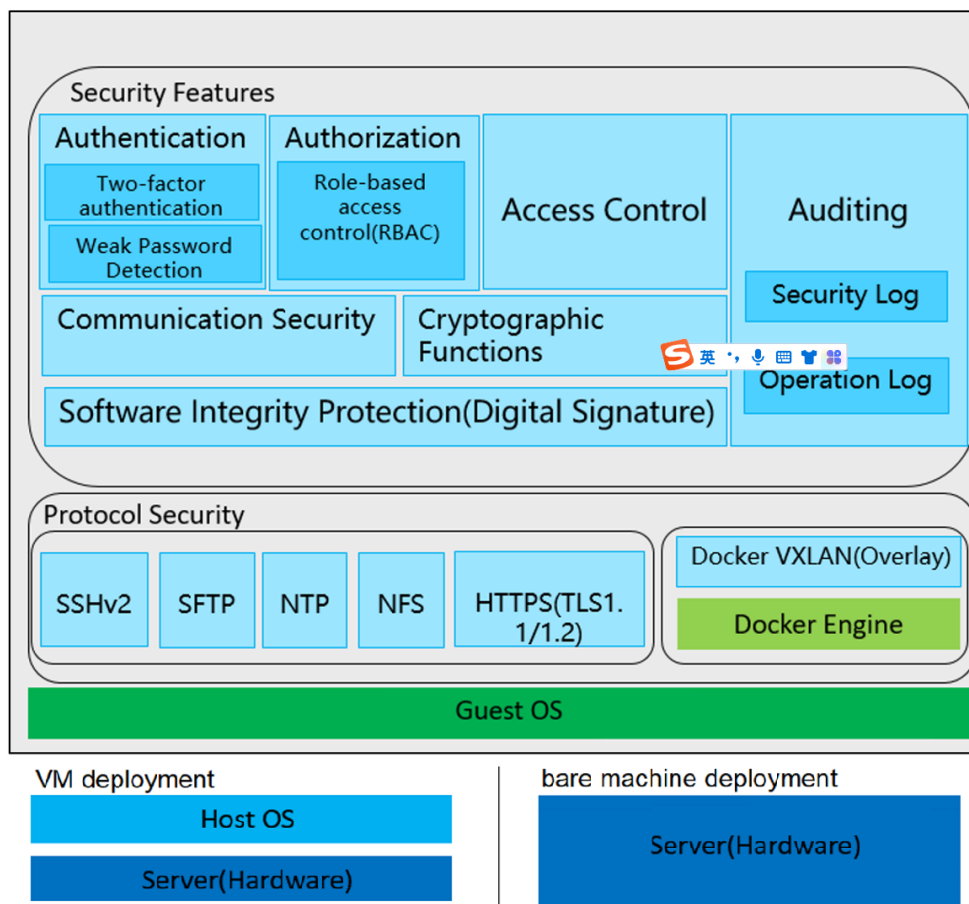


Figure 4: TOE Security functions.

The TOE provides all the security functions, as follows:

Security Features:

- Authentication
- Authorization
- Access Control
- Auditing
- Communication Security
- Cryptographic Functions
- Digital Signature for Software Integrity

Protocol Security:

- SSHv2: provided by open-source software openssl in FusionDirector
- SFTP: provided by open-source software openssl in FusionDirector
- NTP: provided by open-source software ntp in FusionDirector
- NFS: provided by open-source software nfs-utils in FusionDirector
- HTTPS(TLS1.2/1.3): provided by open-source software Nginx in FusionDirector

- Docker swarm overlay network with vxlan: provided by Docker Engine

1.4.3 Summary of Security Features

1.4.3.1 Authentication

The TOE can authenticate administrative users by username and password.

The TOE can perform user enrolment through rest interface or UI only when the user's role is Super administrator.

The TOE provides a local authentication mode, and it can optionally enforce authentication decisions obtained from a LDAP server in the IT environment.

In local authentication mode, accounts and passwords are saved on the local equipment and authenticated using the local account and password by the local equipment during login.

Local authentication also supports two-factor authentication, in two-factor authentication, besides entering username and password, users also need to input secure random codes obtained through mailbox.

In LDAP authentication mode, accounts and passwords are saved on the LDAP server and authenticated by the LDAP server. During login, the accounts and passwords are forwarded to the LDAP server, using the LDAP protocol and the LDAP server checks the validity of accounts and passwords.

After 3 consecutive failed authentication attempts the user account will be blocked for 5 minutes before the user can try to authenticate again.

User authentication is always enforced for virtual terminal sessions via SSH, and SFTP (Secured FTP) sessions. User authentication for access via the console is always enabled. The use of SSH connection is always required for accessing the TOE via Remote Management Terminal (RMT).

The TOE support weak password list. If the password set by user is in the weak password list, the password will not be accepted.

1.4.3.2 Authorization

Authorization indicates that devices assign operation authorities to accounts according to their rights level.

The TOE performs access control using by the group-based authorization framework with predefined role groups for management. Seven user roles by default are offered and can be assigned to individual user accounts.

The TOE manages user privileges by user roles, each user role has different permissions. A user can access a command if the access rights of the command match access rights of the user role.

The seven default user roles are Listed in the following table. Super administrator, Read-only, Device administrator, Firmware administrator, Scope administrator roles can be managed by WebUI. Alarm reporting operator, File transfer operator roles are not displayed on the WebUI.

User Roles/Group	Authority	Security Function
Super administrator	The accounts of this group are used for security management and are authorized to perform all query and configuration operations and assign a user to a different user role.	Authentication Authorization Auditing Communication Security Access Control Cryptographic functions Security Management Software Integrity Protection
Read-only	The accounts of this group have read-only permission for all resources.	Authentication Authorization Auditing Access Control Security Management
Device administrator	This account has server, E9000 management authority, mainly including server status and alarm query, server configuration, firmware upgrade and OS deployment functions.	Authentication Authorization Auditing Access Control Security Management
Firmware administrator	The accounts of this group have server firmware upgrade related permissions.	Authentication Authorization Auditing Access Control Security Management
Scope administrator	The accounts of this group have the relevant permissions of domain operation, read permissions of all resources.	Authentication Authorization Auditing Access Control
File transfer operator	The accounts of this group have permission to transfer files.	Authorization Auditing Access Control
Alarm reporting operator	The accounts of this group have permission to receive BMC alarm events.	Authorization Auditing Access Control

Table 1: Default User roles and authority

All users are assigned corresponding user roles, and all user roles are assigned corresponding operation rights. All authenticated users can execute commands matching user role rights. A user can assign multiple roles and modify them online, and modify scope information online.

1.4.3.3 Access Control

The TOE supports the association of user roles with user IDs, each user role assigns the corresponding operational privileges. The TOE manages user privileges by user roles. The TOE also provides Access Control List (ACL) for filtering incoming information flows to management interfaces. The ACL function protects equipment from network attacks by controlling data of access requests from unauthorized IP addresses and ports. The TOE has the following ACL rules.

Table 1-1 ACL rules

Item	Feature
Limit request rate for single IP address	The TOE limits the frequency of requests from single IP to no more than 20r/s.
Limit request rate for all IP address	The TOE limits the frequency of total requests from external IP to no more than 1000r/s.
URL filtering	The TOE refuses to receive and process messages from URLs configured in URL blacklist. Parse the contents of messages which send by servers managed by FusionDirector. If the context include URL address in the blacklist, this message will be discarded.

1.4.3.4 Auditing

Logs record routine maintenance events of the TOE. Administrators can identify potential security vulnerabilities and risks by investigating logs. In context of security, the TOE provides security logs and operation logs.

Security logs record operation events related to account management, such as login, logout, modification of passwords and addition of accounts.

Operation logs record events related to system configurations, such as modification of equipment IP addresses and addition of services.

All log records contain not only the information on the event itself but also a timestamp and additional information like user ID, source IP, etc.

The TOE provides a Syslog solution to resolve the problem of limited equipment storage space. Both security logs and operation logs are stored locally and can also be stored to the Syslog server.

Logs record can be exported through the FusionDirector Web-based Console page for offline analysis.

Writing to an external audit sever (such as syslog server) can either be done in plaintext (TCP) or protected by using SSL protocol, and default is encrypted. The scope of the certification is restricted to plaintext communication, so the TOE, the external audit server and the path between them needs to be in the same physically protected environment.

If the TOE is connected to an external syslog server and set up to send audit information to it, audit information is sent from the TOE RAM to the external syslog server immediately after the associated event occurred.

1.4.3.5 Communication Security

The TOE enforces communication security by implementing the HTTPS (TLS1.2/1.3) protocol for Web-based Console.

To protect the TOE from eavesdropping and to ensure data transmission security and confidentiality, HTTPS provides:

- Authentication of the TOE by means of RSA 2048bits, PKCS#1 V2.1, RSASSA-PKCS1-v1_5;
- By default, the client authenticates with a username and password. In a scenario with high security requirements, the client can use two-factor authentication;
- AES encryption algorithms, key length support 256bits,128bits;
- Secure cryptographic key exchange.

The TOE enforces communication security by implementing the SSH2 (SSH2.0) protocol for Command-line-based Console.

To protect the TOE from eavesdrop and to ensure data transmission security and confidentiality, SSH2 provides:

- Authentication of the TOE by means of RSA 3072bits, PKCS#1 V2.1, RSASSA-PKCS1-v1_5;
- Authentication of client by username and password;
- AES encryption algorithms;
- Secure cryptographic key exchange.

The port used by SSH is 22 by default. The SSH well-known port 22 can be manually specified a listening port by modifying the SSH configuration file is also implemented, this can effectively reduce attacks.

Beside HTTPS and SSH, SFTP is provided implementing secure FTP based on SSH as communication protocol.

1.4.3.6 Cryptographic Functions

The security features of the TOE require some cryptographic functions. They are defined in chap. 6.7 .

1.4.3.7 Digital Signature for Software Integrity Protection

The TOE provides the ability to verify software validity and prevent the installation of insecure or unauthorized software. FusionDirector uses the digital signature mechanism to protect the software package integrity.

All software versions which are released and ready for production are signed by development before the transfer to production. Software versions are unique. The versions of the released software images and related documents must match the software versions. By verifying the signature and the version information and checking against the version information used for certification of a product, the certified version can be identified. The TOE provides:

- FusionDirector release packages support the OpenPGP digital signature function.
- The integrity of firmware packages on FusionDirector is checked by using the crypto message syntax (CMS) mechanism.

2 CC Conformance Claim

This ST is CC Part 2 conformant [CC], and CC Part 3 conformant [CC]. There are no extended components defined for CC Part 3. The CC version used is 3.1R5.

No conformance to a Protection Profile is claimed.

This ST is conforming to assurance package EAL2+ALC_FLR.1 augmentations.

3 TOE Security Problem Definition

3.1 Asset

The assets to be protected are the information stored, processed or generated by the TOE. Including below:

1. TOE configuration data: which is used for configuration data of security feature and functions.
2. Server username and password: The data which is used by the TOE to identify and authenticate the external entities which interact with the TOE.
3. TOE Crypto data: The data which is used by the TOE for digital signature handling and encryption/decryption purposes.
 - TOE username and password
 - TOE key
4. Audit log: The data which is provided by the TOE during security audit logging
5. Software data: The data which is used by the TOE for software upgrade and configure.
 - Server Firmware
 - Server OS Software
 - Server configuration data
 - FusionDirector Software
6. Necessary network traffic: The network traffic is within the processing range of TOE.

3.2 Threats

FusionDirector mainly implements server batch management functions.

The assumed security threats are listed below:

The information assets to be protected are the information stored, processed or generated by the TOE. Configuration data for the TOE, TSF data (such as user account information and

passwords, audit records, etc.) and other information that the TOE facilitates access to (such as system software, firmware software) are all considered part of information assets.

As a result, the following threats have been identified:

T.UnauthenticatedAccess

An attacker that is not an authenticated user of the TOE gains access to the TOE and modifies TOE configuration data, Server configuration data, firmware, OS software, or gets username and password without permission.

- T.UnauthenticatedAccess
 - Threat agent: An attacker that is not a user of the TOE.
 - Asset: TOE configuration data
 - Adverse action: An attacker that did not authenticate to the TOE gets access to the TOE and by that could be able to modify TOE configuration data without permission (compromising TOE integrity and availability).
- T.UnauthenticatedAccess
 - Threat agent: An attacker that is not a user of the TOE.
 - Asset: Server configuration data
 - Adverse action: An attacker that did not authenticate to the TOE gets access to the TOE and by that could be able to modify or delete the server configuration data, causing the server to operate abnormally and fail to provide services.
- T.UnauthenticatedAccess
 - Threat agent: An attacker that is not a user of the TOE.
 - Asset: TOE username and password
 - Adverse action: An attacker that did not authenticate to the TOE gets access to the TOE and by that could be able to do the following operations:
 - ◆ The abnormal operation of the server managed by the FusionDirector (such as powering down, restarting, and modifying the server configuration) causes the services carried on the server to fail to run normally.
 - ◆ The attacker illegally obtains server information by calling the FusionDirector interface.
 - ◆ Modify or delete the firmware file or OS image file, resulting in abnormal firmware upgrade or OS deployment.
 - ◆ The attacker logs in to the FusionDirector to perform the attack (such as deleting the process and modifying the configuration). As a result, the FusionDirector runs abnormally and cannot provide server management functions.
- T.UnauthenticatedAccess
 - Threat agent: An attacker that is not a user of the TOE.
 - Asset: Server username and password(including BMC、 Switch、 IRM , etc.)
 - Adverse action: An attacker obtains the server software username and password without permission, and uses these username passwords to access the server-related software to initiate an attack on the server, causing the server to function abnormally.

T.UnauthorizedAccess

A user of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for. By that he could modify TOE configuration data, Server configuration data, firmware, OS software, or gets username and password without permission.

- T.UnauthorizedAccess
 - Threat agent: Unauthorized personnel: i.e. authenticated user with insufficient privileges.
 - Asset: TOE configuration data
 - Adverse action: A user with insufficient privileges gets access to TOE security functions which would require additional privileges. By that he could be able to modify TOE configuration data without permission (compromising TOE integrity and availability), causing FusionDirector to function abnormally.
- T.UnauthorizedAccess
 - Threat agent: Unauthorized personnel: i.e. authenticated user with insufficient privileges.
 - Asset: Server configuration data
 - Adverse action: A user with insufficient privileges gets access to TOE security functions which would require additional privileges. By that he could be able to modify server configuration data without permission (compromising server integrity and availability), causing the server to function abnormally.
- T.UnauthorizedAccess
 - Threat agent: Unauthorized personnel: i.e. authenticated user with insufficient privileges.
 - Asset: TOE username and password
 - Adverse action: A user with insufficient privileges gets access to TOE security functions which would require additional privileges. By that he could be able to get TOE username password without permission (Override access), As a result, a user can illegally call the FusionDirector API interface.
- T.UnauthorizedAccess
 - Threat agent: Unauthorized personnel: i.e. authenticated user with insufficient privileges.
 - Asset: Server username and password(including BMC、 Switch、 IRM , etc.)
 - Adverse action: A user with insufficient privileges gets access to TOE security functions which would require additional privileges. By that he could be able to get server username password without permission (Override access), As a result, a user can illegally access the server software.
- T.UnauthorizedAccess
 - Threat agent: Unauthorized personnel: i.e. authenticated user with insufficient privileges.
 - Asset: TOE key

- Adverse action: A user with insufficient privileges gets access to TOE security functions which would require additional privileges. By that he could be able to get TOE key without permission (Override access), As a result, a user can use the key to decrypt the ciphertext of sensitive data.
- T.UnauthorizedAccess
 - Threat agent: Unauthorized personnel: i.e. authenticated user with insufficient privileges.
 - Asset: Audit log
 - Adverse action: A user with insufficient privileges gets access to TOE security functions which would require additional privileges. By that he could be able to modify or delete TOE log without permission (Override access), As a result, a user can repudiate what they have done to TOE.
- T.UnauthorizedAccess
 - Threat agent: Unauthorized personnel: i.e. authenticated user with insufficient privileges.
 - Asset: FusionDirector Software, Server Firmware, and Server OS Software
 - Adverse action: A user with insufficient privileges gets access to TOE security functions which would require additional privileges. By that he could be able to modify FusionDirector Software, Firmware, and OS Software without permission (Override access), As a result, a user can run illegal, tampered software, causing the FusionDirector to function abnormally or causing the server to function abnormally.

T.Repudiation

An attacker refuses to acknowledge the operation that has been performed on the TOE.

- Threat agent: An attacker in the management network.
- Asset: Server configuration data, Server Firmware and Server OS Software
- Adverse action: Attackers may refuse to admit log on to the system and illegally modify configuration data, firmware and server OS image files.

T.Tampering

An attacker tampers critical data of TOE, such as configuration data, audit log, firmware and server OS image files integrity.

- Threat agent: An attacker in the management network.
- Asset: Server configuration data, audit log, Server Firmware and Server OS Software
- Adverse action: Attackers may log on to the system and illegally modify configuration data, audit log, firmware and server OS image files.

T.InformationDisclosure

An attacker gets sensitive data of TOE without permission, such as password, key, and uses the acquired sensitive information to disguise as a legitimate user and perform an attack operation.

- Threat agent: An attacker in the management network.
- Asset: TOE Crypto data

- Adverse action: Attackers acquire sensitive information, such as passwords, keys, and use the acquired sensitive information to further attack the system. For example, after acquiring passwords, they can log into the system and perform illegal operations. After acquiring keys, they can use keys to decrypt the ciphertext and obtain plaintext data.

T.Eavesdrop

An eavesdropper (remote attacker) in the management network served by the TOE is able to intercept, and potentially modify or re-use information assets which are not protected against modification and disclosure that are exchanged between TOE and Web-based Console, or TOE and server.

- Threat agent: An eavesdropper (remote attacker) in the management network.
- Asset: TOE Crypto data, Audit log, Server username and password
- Adverse action: Intercept, and potentially modify or re-use information from network traffic which is exchanged between TOE and Web-based Console, or TOE and server. By this confidentiality and integrity of the data transmitted could be compromised.

T.UnwantedNetworkTraffic

Unnecessary network traffic sent to the TOE will cause the TOE's processing capacity for incoming network traffic to be consumed thus fails to process traffic expected to be processed, As a result, FusionDirector does not provide server management functions properly.

This may further cause the TOE to fail to respond to system control and security management operations.

- Threat agent: An attacker that is not a user of the TOE.
- Asset: Necessary network traffic.
- Adverse action: The attacker could send too much unnecessary network traffic to exhaust the resources of the TOE and by that compromising server management capability of the TOE. The attacker may send too much unnecessary network traffic to exhaust the resources of the TOE, and by that causing the TOE to fail to respond properly to legitimate requests (TOE availability).

3.3 Assumptions

A.NetworkSegregation

It is assumed that the operational environment provides segregation of networks by deploying the management interface in TOE into an independent local network.

A.CorrectWorkingOS

It is assumed that the Host OS used by FusionDirector should be installed and working normally. It is also assumed that the Host OS provide stable system services. The Host OS is a standard Linux operating system which is out of the TOE.

A.CorrectWorkingNTPServer

It is assumed that external clock used by the NTP client is reliable.

A.NoEvil

It is assumed that personnel working as authorized administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A. Correct Working Hardware

It is assumed that the TOE and its operational environment such as CPU, memory, hard disk storage, network port and clock source can work normally. It is also assumed that the local management network, including the server BMC, iRM, syslog server, and locally attached management terminals (LMT) together with all related communication lines are operated in the same physically secured environment as the TOE.

A. Physical Protection

It is assumed that the TOE is protected against unauthorized physical access.

4 Security Objectives

4.1 Objectives for the TOE

The following objectives must be met by the TOE:

O.Authentication

The TOE shall support the authentication of users by local username and password. This applies to local (Local Management Terminal, LMT) and remote access (Remote Management Terminal, RMT). The authentication mechanisms shall allow identifying users. This information shall also be provided to other security functions if required (e.g. user identities for audit functionality).

O.Authorization

The TOE shall implement different authorization levels that can be assigned to users in order to restrict the functionality that is available to individual users.

O.Audit

The TOE shall provide functionality to generate audit records for security-relevant events.

O.Integrity

The TOE shall provide functionality to protect the integrity of stored critical data, such as TOE configuration data, Server configuration data, audit log, firmware and server OS image files integrity.

O.Encryption

The TOE shall provide functionality to protect Sensitive data with encryption, such as TOE Crypto data.

O.Communication

The TOE must implement logical protection measures for network communication between the TOE and Remote Management Terminal (RMT) from the operational environment. These protection measures shall include device authentication and the use of a secure communication protocol.

O.SecurityManagement

The TOE shall provide functionality to securely manage security functions provided by the TOE. This includes:

- Account and password policy configuration
 - Maximum number of accounts created by the system
 - The length of lockout after a user failed to log in
 - Account Name Minimum, Maximum Length Limit
 - Password cannot be repeated with historical passwords
 - Maximum number of consecutive failed authentication attempts allowed before the account is locked
 - Minimum time limit between two password modifications
 - The password is valid within a specified period, and will expire after the period
- Session policy configuration
 - Session Timeout Period
 - Maximum Number of Sessions Allowed by the System
- Management of user accounts and authorization (including two-factor authentication configuration).
- Definitions and maintenance of managed objects groups and command groups.
- Management of secure communication channels.
- Configuration of ACL functionality by authorized users.

O.AccessControl

The TOE provides Access Control List (ACL) for filtering incoming information flows to management interfaces. The ACL function protects equipment from network attacks by controlling data of access requests from unauthorized IP addresses and ports.

4.2 Objectives for the Operational Environment

OE.NetworkSegregation

The operational environment shall separate the interfaces for Server Management purposes from the ETH interface to remote administration. The ETH port shall not be connected to a company's business network or public network, but only to a separate sub-network especially separated from these other networks where forwarding by the TOE takes place. The business network should isolate from management network to ensure business security. The management network and business network does not allow access from the Internet directly which need to control access policy through VPN.

OE.Person

Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE. This includes instruction to follow and abide the instructions provided by the TOE documentation.

OE.CorrectWorkingOS

The Host OS used by FusionDirector is a standard Linux operating system should be installed and working correctly, which include the essential provisions of power, possibly clock frequencies and other essential physical interfaces.

OE.CorrectWorkingNTPServer

NTP Server Connected by FusionDirector works normally which include accurate clock source.

OE.CorrectWorkingHardware

The underlying hardware on which FusionDirector is installed should work properly which include CPU, memory, hard disk storage, network port and clock source.

OE.PhysicalProtection

The TOE (i.e., the complete system including attached interfaces) shall be protected against unauthorized physical access.

4.3 Security Objectives Rationale

4.3.1 Coverage

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

Objective	Threat
O.Authentication	T.UnauthenticatedAccess
O.Authorization	T.UnauthorizedAccess
O.Audit	T.UnauthenticatedAccess T.UnauthorizedAccess T.Repudiation
O.Integrity	T.Tampering
O.Encryption	T.InformationDisclosure
O.Communication	T.Eavesdrop
O.AccessControl	T.UnwantedNetworkTraffic
O.SecurityManagement	T.UnauthenticatedAccess T.UnauthorizedAccess

	T.Eavesdrop T.UnwantedNetworkTraffic
--	---

Table 2: Mapping Objectives to Threats

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

Environmental Objective	Threat / Assumption
OE.NetworkSegregation	A.NetworkSegregation
OE.CorrectWorkingOS	A.CorrectWorkingOS
OE.CorrectWorkingNTPServer	A.CorrectWorkingNTPServer
OE.Person	A.NoEvil
OE.CorrectWorkingHardware	A.CorrectWorkingHardware
OE. PhysicalProtection	A.PhysicalProtection

Table 3: Mapping Objectives for the Environment to Threats, Assumptions

4.3.2 Sufficiency

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

Threat	Rationale for security objectives to remove Threats
T.UnauthenticatedAccess	<p>The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication).</p> <p>Authentication mechanisms can be configured by users with sufficient user level (O.SecurityManagement).</p> <p>Detected attempts of unauthenticated access are regarded as security relevant events which lead to the generation of a related audit record (O.Audit).</p>
T.UnauthorizedAccess	<p>The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization).</p> <p>Access control mechanisms (including user levels and command levels) can be configured by users with sufficient user level (O.SecurityManagement).</p> <p>Detected attempts of unauthorized access are regarded as security relevant events which lead to the generation of a related audit record</p>

	(O.Audit).
T.Repudiation	The threat of repudiation is countered by requiring the TOE to implement logging function (O.Audit).
T.Tampering	The threat of tampering is countered by requiring the TOE to implement data integrity checking function (O.Integrity).
T.InformationDisclosure	The threat of information disclosure is countered by requiring the TOE to implement data encryption function (O.Encryption).
T.Eavesdrop	The threat of eavesdropping is countered by requiring communication security via HTTPS or SSHv2 for communication between RMT and the TOE (O.Communication). Management of secure communication channels can be performed by users with sufficient user level (O.SecurityManagement).
T.UnwantedNetworkTraffic	ACL functionality can be used to deny unnecessary network traffic to enter or pass the TOE.(O.AccessControl) ACL functionality can be configured by users with sufficient user level (O.SecurityManagement)

Table 4: Sufficiency analysis for threats

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

Assumption	Rationale for security objectives
A.NetworkSegregation	The assumption that the TOE is not accessible via the application (or public) networks hosted by the networking device is addressed by requiring just this in OE.NetworkSegregation.
A.CorrectWorkingOS	The assumption that the OS used by FusionDirector shall work correctly is expressed by a corresponding requirement in OE. CorrectWorkingOS.
A.CorrectWorkingNTPServer	The assumption that the NTP Server Connected by FusionDirector works normally is expressed by a corresponding requirement in OE. CorrectWorkingNTPServer.

A.NoEvil	The assumption that the administrators of the TOE are not careless, willfully negligent, or hostile is addressed in OE.Person.
A.CorrectWorkingHardware	The assumption that the underlying hardware is working correctly is expressed by a corresponding requirement in OE.CorrectWorkingHardware.
A. PhysicalProtection	The assumption that the TOE shall be protected against unauthorized physical access is expressed by a corresponding requirement in OE.PhysicalProtection.

Table 5: Sufficiency analysis for assumptions

4.4 TSF and Non-TSF Data

All data from and to the interfaces available on the TOE is categorized into TSF data and non-TSF data. The following is an enumeration of the subjects and objects participating in the policy.

TSF data:

- User account data, including the following security attributes:
 - User credentials.
 - Locally managed passwords.
 - Locally managed access levels.
- Audit configuration data.
- Audit records.
- Configuration data of security feature and functions.
- Key used in sensitive data encryption.

Non-TSF data:

- Security-independent data in TOE (e.g. operation log, micro-service running status).
- Server information (such as CPU, memory, hard disk, fan, etc.).

5 Security Requirements

5.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement
- underlined text 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/Identifier indicates an element of the iteration, where Identifier distinguishes the different iterations.

5.2 Definition of Security Policies

To avoid redundancy in the definition of SFRs, in this chapter the security policies are defined that have to be fulfilled by the TOE.

5.2.1 Access Control Policy

The access control policy is implemented through authentication and access control mechanisms as described in chap. 1.4.3.1 and 1.4.3.3 respectively.

The TOE access control policy defines the following subjects, objects and attributes:

Subjects:

- Users

Objects:

- Commands

Information security attributes:

- User roles
- Scope

Application Note: Please refer to the application note in section 5.3.5.1 (FMT_MOF.1) for detailed meaning of "Scope".

5.3 TOE Security Functional Requirements

5.3.1 Security Audit (FAU)

5.3.1.1 FAU_GEN.1 Audit Data Generation

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

- a) ~~Start up and shut down of the audit functions~~
- b) All auditable events for the *not specified* level of audit; and
- c) **The following auditable events:**

- i. user activity**

- 1. Login, logout**

- ii. Management of user accounts**

- 1. Add, delete, modify (refers to account authority)**

- 2. Password change (by the user himself or administrator)**

- 3. User Locking and Unlocking**

- 4. User role change**

- 5. Security Policy Configuration**

- iii. Management of scope**

- 1. Add, delete, modify**

- iv. Security policy modification**

- v. Certificate management**

- vi. System management**

- 1. Operation requests (i.e. configuration of the device, FusionDirector update, firmware update, OS image deployment)**

- vii. Log management**

- 1. log policy modification**

Application Note: Changes to user levels are covered by **Management of user accounts**. Changes to command levels are covered by **Management of scope**. The start-up and shut down of audit functions does not apply as the audit functionality shall be active immediately after start-up and remains active all times. This means that even the administrator shall not have a possibility to stop or shut down the audit functionality.

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 ID (if applicable)**, and **CLI command name (if applicable)**.

Application Note: All external interfaces calls are logged, and the log content includes at least the following information:

- a) The time of the event;
- b) User ID;
- c) Access the address or identity of the originator (e.g. associated terminals, ports, network addresses, communication devices, etc.);
- d) Event type;
- e) The name of the resource being accessed;
- f) The result of the event.

5.3.1.2 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.

5.3.1.3 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.

5.3.1.4 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* unauthorized modifications to the stored audit records in the audit trail.

5.3.1.5 FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The TSF shall **delete the oldest audit data** if the audit trail exceeds **100 thousand**.

Application Note: The audit data are written to data base, or external audit servers (if configured), audit number in data base exceeds 1 million the oldest audit data is overwritten.

5.3.2 Cryptographic Support (FCS)

5.3.2.1 FCS_COP.1/AES Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **symmetric decryption and encryption** in accordance with a specified cryptographic algorithm **AES operating in the following mode**.

GCM mode, and cryptographic key sizes **256bits** that meet the following: [FIPS 197], [FIPS SP 800-38D]

GCM mode, and cryptographic key sizes **128bits** that meet the following: [FIPS 197], [FIPS SP 800-38D]

CTR mode, and cryptographic key sizes **128bits** that meet the following: [FIPS 197], [FIPS SP 800-38A]

CTR mode, and cryptographic key sizes **192bits** that meet the following: [FIPS 197], [FIPS SP 800-38A]

CTR mode, and cryptographic key sizes **256bits** that meet the following: [FIPS 197], [FIPS SP 800-38A]

CBC mode, and cryptographic key sizes **256bits** that meet the following: [FIPS 197], [FIPS SP 800-38A]

CBC mode, and cryptographic key sizes **128bits** that meet the following: [FIPS 197], [FIPS SP 800-38A]

Application Note:

AES-128/192/256 in **CTR mode** is used for encryption and decryption within SSH communication.

aes128-gcm@openssh.com/aes256-gcm@openssh.com/chacha20-poly1305@openssh.com is used for encryption and decryption within SSH communication.

AES-128/256 in **GCM mode** is used for encryption and decryption within TLS communication.

AES-128/256 in **CBC mode** is used for encryption and decryption within TLS communication.

AES-256 in **CBC mode** is used for encryption and decryption within password encryption before storage in non-volatile memory.

5.3.2.2 FCS_COP.1/RSA Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **asymmetric authentication** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **2048bits** and **3072bits** that meet the following: **RSA Cryptography Standard ([PKCS#1 V2.1], RSASSA-PKCS1-v1_5 for SSH)**

Application Note:

RSA with key size of 2048bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 together with SHA256 is used for asymmetric authentication of the TLS._

RSA with key size of 2048bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 together with SHA256 / SHA384 / SHA512 is used for verification of a digital signature of the software package.

RSA with key size of 3072bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 together with SHA256 is used for asymmetric authentication of the SSH.

5.3.2.3 FCS_COP.1/HMAC-SHA1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **data integrity generation and verification** in accordance with a specified cryptographic algorithm **HMAC-SHA1** and cryptographic key sizes **160 bits** that meet the following: [RFC 2104], [FIPS 198-1]

Application Note: HMAC-SHA1 is used for integrity protection of SSH communication.

5.3.2.4 FCS_COP.1/HMAC-SHA2 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **data integrity generation and verification** in accordance with a specified cryptographic algorithm **HMAC-SHA2** and cryptographic key sizes **256/512 bits** that meet the following: [RFC 2104], [FIPS 198-1]

Application Note: HMAC-SHA2-256/ HMAC-SHA2-512 is used for integrity protection of SSH communication.

5.3.2.5 FCS_COP.1/SHA256 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **hashing** in accordance with **SHA256** and cryptographic key sizes **None** that meet the following: [FIPS 180-4]

Application Note: SHA256 is used in TLS communication.

5.3.2.6 FCS_COP.1/SHA384 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **hashing** in accordance with **SHA384** and cryptographic key sizes **None** that meet the following: [FIPS 180-4]

Application Note: SHA384 is used in TLS communication.

5.3.2.7 FCS_COP.1/PBKDF2 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **hashing** in accordance with **PBKDF2 (HMAC-SHA256)** and cryptographic key sizes **None**, Iteration number is 10000 that meet the following: [RFC2898], [PKCS #5]

Application Note: PBKDF2 is used for hashing passwords before storage in non-volatile memory.

5.3.2.8 FCS_CKM.1/DH Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **diffie-hellman-group14-sha1/diffie-hellman-group-exchange-sha256/diffie-hellman-group-exchange-sha1/ECDHE RSA/DHE RSA** and specified cryptographic key sizes **128/256 bits** that meet the following: [NIST Special Publication 800-56A], [RFC 4250], [RFC 4253], [RFC 3526], [RFC 4346], [RFC 5246], [RFC 4492], [PKCS#3], [RFC 5246], [RFC 4346] and [RFC 4492] for SSH/TLS.

Application Note: When establish SSH communications, the TOE generates a shared secret value with the peer during the DH key agreement use diffie-hellman-group14-sha1/diffie-hellman-group-exchange-sha256/ diffie-hellman-group-exchange-sha1 algorithm. The shared secret value is used to derive session keys used for encryption and decryption, and generation

and verification of integrity protection information for SSH communication. The key generation is performed according to [RFC 4250], [RFC 4253], [RFC 3526].

When establish TLS communications, the TOE generates a shared secret value with the peer during the DH key agreement use ECDHE_RSA/DHE_RSA algorithm. RSA private key sizes is 2048bit which used to exchange key used for encryption and decryption, and generation and verification of integrity protection information for TLS communication. The key generation is performed according to [RFC 4346], [RFC 5246], [RFC 4492].

5.3.2.9 FCS_CKM.1/RSA Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **2048bits** that meet the following: [FIPS 186-4], chap. 5.1., **RSA key pairs for RSASSA-PKCS1-V1_5 using CRT**.

Application Note: RSA with key size of 2048bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 together with SHA256 is used for asymmetric authentication of the SSH and TLS.

5.3.2.10 FCS_CKM.4/RSA Cryptographic Key Destruction

FCS_CKM.4.1/RSA The TSF shall destroy cryptographic (**RSA**) keys in accordance with a specified cryptographic key destruction method **overwriting with 0** that meets the following: **none**

Application Note: This SFR was refined to RSA keys only. The destruction mechanism has to be triggered manually.

5.3.3 User Data Protection (FDP)

5.3.3.1 FDP_ACC.1 Subset Access Control

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

[Subject: Super administrator;

Objects: all resource (Including server resources and FusionDirector software resources);

Operation: Read access / write access]

[Subject: Read-only;

Objects: all resource (Including server resources and FusionDirector software resources);

Operation: Read access]

[Subject: Device administrator;

Objects: Server resource (Including the server board, chassis, management board, and switch board.);

Operation: Read access / write access]

[Subject: Firmware administrator;
Objects: firmware;
Operation: Read access / write access]

[Subject: Scope administrator;
Objects: Scope resource;
Operation: Read access / write access]

[Subject: File transfer operator;
Objects: files;
Operation: Read access]

[Subject: Alarm reporting operator;
Objects: event messages;
Operation: Read access]

5.3.3.2 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:

- a) **list of subjects and objects which are defined in section 5.3.3.1 FDP_ACC.1.**
- b) **users and their following security attributes:**
 - i. **user account**
 - ii. **user roles**
 - iii. **scope of user binding**
- c) **commands and their following security attributes:**
 - i. **Operation command**
 - ii. **Operation resource**

Application Note: For every command there is an associated user roles, That is, to associate each command with user roles and determine the permissions that must be granted to access each command.

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

- 1 **Only authorized users are permitted access to commands and feature.**
- 2 **Users can be configured with different user roles to control the device access permission.**

- 3 **There are seven user roles including Super administrator, Read-only, Device administrator, Firmware administrator, Scope administrator, File transfer operator, Alarm reporting operator.**
- 4 **Each user role corresponds to different command. Users gain permission to execute commands by associating user roles.**
- 5 **Each user binds his own operation privileges by associating user roles, that is, commands that can be executed; each user binds a set of resources that can be operated by associating scopes.]**

FDP_ACF.1.3 The TSF shall explicitly authorize 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**.

5.3.3.3 FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **the authentication information of SSH, HTTPS, SFTP and Configuration data and audit log**.

FDP_DAU.1.2 The TSF shall provide **Super administrator** with the ability to verify evidence of the validity of the indicated information.

5.3.3.4 FDP_DAU.2 Data Authentication with Identity of Guarantor

FDP_DAU.2.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **software version, firmware version**.

FDP_DAU.2.2 The TSF shall provide **Super administrator, Firmware administrator** with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

5.3.3.5 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the **information control policy** based on the following rules

- a) **The TOE limit request rate for single IP address.**
- b) **The TOE limit request rate for all IP address.**
- c) **The TOE refuses to receive and process messages from the blacklist by configuring the URL blacklist. Parse the contents of messages which send by servers managed by FusionDirector. If the context include URL address in the blacklist, this message will be discarded.**

5.3.3.6 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the **information control policy** based on the following types of subject and information security attributes:

Subject: Users

Information security attributes:

Packet characteristic:

- URL
- Request frequency

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **Network traffic is matched the configured policies of TOE.**

The specific information flow control rules associated with each policy are as described in chap. 1.4.3.3.

FDP_IFF.1.3 The TSF shall enforce the **information control policy based on the following rules:**

- a) **The TOE limit request rate for single IP address.**
- b) **The TOE limit request rate for all IP address.**
- c) **The TOE refuses to receive and process messages from the blacklist by configuring the URL blacklist. Parse the contents of messages which send by servers managed by FusionDirector. If the context include URL address in the blacklist, this message will be discarded.**

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **none.**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **[For ACL feature, packets that match configured ACL with action “deny” are dropped]**

5.3.3.7 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: **all resource (Including server resources and FusionDirector software resources).**

Application Note: Whenever a Trusted Path is terminated for whatever reason, all temporary session keys are erased from the volatile memory by the post-processing routines associated with the Trusted Path. These session keys are generated by FCS_CKM.1/DH and are used by FCS_COP.1/AES, FCS_COP.1/RSA FCS_COP.1/HMAC-SHA1, FCS_COP.1/HMAC-SHA2, FCS_COP.1/SHA256 and FCS_COP.1/SHA384, respectively.

5.3.4 Identification and Authentication (FIA)

5.3.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within [3 to 10]* unsuccessful authentication attempts occur related to **since the last successful authentication of the indicated user identity.**

Application Note: The TSF detects the number of times the user enters the wrong password continuously, and locks the user when the maximum number of settings is reached. The number of errors can be configured, at least 3 times.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed*, the TSF shall **terminate the session of the user trying to authenticate and block the user account for authentication for at least 5 minutes.**

Application Note: When the defined number of unsuccessful authentication attempts is exceeded, the TSF terminates the user attempting to authenticate and locks the user account for at least 5 minutes. The lock time can be configured for at least 5 minutes.

5.3.4.2 FIA_ATD.1 User attribute definition

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

- a) **User ID**
- b) **User level**
- c) **PBKDF2(The hash function is SHA256) hashes of passwords**
- d) **Temporary blocking time for user accounts after unsuccessful authentication attempts**
- e) **Time when users are logging in and logging off.**

5.3.4.3 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.

Application Note: Authentication is possible by username and password._

5.3.4.4 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.

Application Note: Authentication is possible by username and password. The user is identified by his username if he is able to successfully authenticate with his username and corresponding password.

5.3.5 Security Management (FMT)

5.3.5.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the behavior, determine the behavior* of the functions **identified in FMT_SMF.1 to users with sufficient user roles as defined in Table 6 in section 5.3.5.7.**

Application Note: Access control of the TOE works as follows: All user are assigned to user roles and scope. User roles are used to control the set of commands that can be executed, and scopes are used to control the set of operating objects. Users can only execute a command if their associated user roles match the permissions of this command, and operational resources are within the scope that the user can operate on. The management of user roles also depends on this access control mechanism. TOE has seven user roles by default, all commands are registered in seven default user roles.

5.3.5.2 FMT_MSA.1/ ACFATD Management of Security Attributes

FMT_MSA.1.1/ACFATD The TSF shall enforce the **authentication and authorization requirements defined by FMT_SMR.1 and FIA_UID.2 and FIA_UAU.2** to restrict the

ability to *query, modify* the security attributes **identified in FDP_ACF.1 and FIA_ATD.1** to **users with sufficient user roles as defined in Table 6 in section 5.3.5.7.**

Application Note: See Application Note for FMT_MOF.1 for clarification.

5.3.5.3 FMT_MSA.1/ IFF Management of Security Attributes

FMT_MSA.1.1/IFF The TSF shall enforce the **Super administrator** to restrict the ability to *modify, delete* the security attributes **identified in FDP_IFF.1** to **users with sufficient user roles.**

5.3.5.4 FMT_MSA.3/ ACFATD Static Attribute Initialization

FMT_MSA.3.1/ACFATD The TSF shall enforce the **authentication and authorization requirements defined by FMT_SMR.1 and FIA_UID.2 and FIA_UAU.2** to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ACFATD The TSF shall allow **users with sufficient user roles as defined in Table 6 in section 5.3.5.7** to specify alternative initial values to override the default values when an object or information is created.

5.3.5.5 FMT_MSA.3/ IFF Static attribute initialization

FMT_MSA.3.1/IFF The TSF shall enforce the **Super administrator** to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/IFF The TSF shall allow **users with sufficient user roles as defined in Table 6 in section 5.3.5.7** to specify alternative initial values to override the default values when an object or information is created.

5.3.5.6 FMT_SMF.1 Specification of Management Functions

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

- a) **Authentication, authorization**
- b) **Accounts management**
- c) **Scopes management**
- d) **Query audit records**
- e) **Configure the Password Policy**
- f) **Configure the Account Policy**
- g) **Configure Session Policy**
- h) **Configure audit functionality including output host for audit data.**
- i) **Certificates management**

5.3.5.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: **users with associated user roles, which are described in the following table.**

User Roles/Group	Authority	Security Function
Super administrator	The accounts of this group are used for security management and are authorized to perform all query and configuration operations and assign a user to a different user role.	Authentication Authorization Auditing Communication Security Access Control Cryptographic functions Security Management Software Integrity Protection
Read-only	The accounts of this group have read-only permission for all resources.	Authentication Authorization Auditing Access Control Security Management
Device administrator	This account has server, E9000 management authority, mainly including server status and alarm query, server configuration, firmware upgrade and OS deployment functions.	Authentication Authorization Auditing Access Control Security Management
Firmware administrator	The accounts of this group have server firmware upgrade related permissions.	Authentication Authorization Auditing Access Control Security Management
Scope administrator	The accounts of this group have the relevant permissions of domain operation, read permissions of all resources.	Authentication Authorization Auditing Access Control
File transfer operator	The accounts of this group have permission to transfer files.	Authorization Auditing Access Control
Alarm reporting operator	The accounts of this group have permission to receive BMC alarm events.	Authorization Auditing Access Control

Table 6: Default User roles and authority

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

Application Note: See Application Note for FMT_MOF.1 for clarification.

5.3.6 Protection of the TSF (FPT)

5.3.6.1 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note: The reliable time stamps are based on the information of the real time clock (RTC) of the hardware. The RTC itself is not part of the TOE. The time stamps rely on the correct operation of the RTC of the underlying hardware as defined in OE.CorrectWorkingHardware.

TOE can also connect to the NTP server and get reliable time stamps from the NTP server which defined in OE. CorrectWorkingNTPServer.

5.3.7 TOE access (FTA)

5.3.7.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after **a time interval of user inactivity which can be configured by a user with sufficient user level.**

Application Note: When the session is idle for more than a certain period of time, the TSF terminates the current session, which is configurable by the user with administrator privileges, a minimum of 5 minutes, a maximum of 60 minutes, and a default of 5 minutes.

5.3.7.2 FTA_TSE.1 TOE session establishment

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

- a) **Authentication failure**

5.3.8 Trusted Path/Channels (FTP)

5.3.8.1 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 *initial user authentication*

Application Note:

- a) To establish a trusted path, the TLS protocol shall be used that complies with RFCs 5246 [RFC 5246] and 4346 [RFC 4346]. For Key Exchange the ECDHE, DHE, RSA algorithm shall be used which is in agreement with [RFC 5246], [RFC 4346] and [RFC 4492]. For authentication the RSA algorithm shall be used which is in agreement with [RFC 2437] and [RFC 8017]. For encryption the AES-128/256 algorithm (GCM or CBC mode) shall be used which is in agreement with [RFC 3268] and [RFC 5288]. For Data Integrity, the HMAC-SHA1, HMAC-SHA2-256 or HMAC-SHA2-384 algorithm shall be used which is in agreement with [RFC 4634] and [RFC 3174].

- b) To establish a trusted path, the SSH protocol shall be used that complies with RFCs 4251 [RFC 4251], 4252 [RFC 4252], 4253 [RFC 4253] and 4254 [RFC 4254]. For encryption the AES-128 algorithm (CTR mode) shall be used which is in agreement with [RFC 4253]. For Data Integrity, the HMAC-SHA1, HMAC-SHA2-256 or HMAC-SHA2-512 algorithm shall be used which is in agreement with [RFC 4253]. For Key Exchange the diffie-hellman-group1-sha1, diffie-hellman-group1-sha256 algorithm shall be used (AES encryption) which is in agreement with [RFC 4253]. For client user authentication the TOE shall support password authentication according to chap. 9.4.5 [RFC 4251] and chap. 8 [RFC 4252], respectively. Server authentication is performed using RSA according to chap. 6.6 [RFC 4253], ssh-rsa. In addition, SFTP (i.e. FTP based on SSH protocol) is supported for secure file transfer. SSH communication is sometimes also referred to as ‘STelnet’.

5.4 Security Functional Requirements Rationale

5.4.1 Coverage

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

Security Functional Requirements	Objectives
FAU_GEN.1	O.Audit
FAU_GEN.2	O.Audit
FAU_SAR.1	O.Audit
FAU_STG.1	O.Audit
FAU_STG.3	O.Audit
FCS_COP.1/PBKDF2	O.Encryption
FCS_COP.1/AES, FCS_COP.1/SHA256	O.Communication O.Encryption
FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA1, FCS_COP.1/HMAC-SHA2, FCS_COP.1/SHA384	O.Communication
FCS_CKM.1/DH, FCS_CKM.1/RSA	O.Communication
FCS_CKM.4/RSA	O.Communication
FDP_ACC.1	O.Authorization
FDP_ACF.1	O.Authorization
FDP_DAU.1	O.Communication

	O.Integrity O.Audit
FDP_DAU.2 FCS_COP.1/RSA	O.Integrity
FDP_IFC.1	O.AccessControl
FDP_IFF.1	O.AccessControl
FDP_RIP.1	O.Communication
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication O.Authorization
FIA_UAU.2	O.Authentication
FIA_UID.2	O.Authentication O.Authorization
FMT_MOF.1	O.Authorization
FMT_MSA.1.1/ACFATD	O.Authorization
FMT_MSA.3/ ACFATD	O.Authorization
FMT_MSA.1.1/IFF	O.Authorization O.AccessControl
FMT_MSA.3/ IFF	O.Authorization O.AccessControl
FMT_SMF.1	O.SecurityManagement O.Authentication O.Authorization
FMT_SMR.1	O.Authorization O.SecurityManagement
FPT_STM.1	O.Audit

FTA_SSL.3	O.Communication
FTA_TSE.1	O.Communication
FTP_TRP.1	O.Authentication O.Communication

Table 7: Mapping SFRs to objectives

5.4.2 Sufficiency

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

Security objectives	Rationale
O.Authentication	<p>User authentication is implemented by FIA_UAU.2, supported by individual user identification in FIA_UID.2. The requirements on necessary user attributes (passwords) are addressed in FIA_ATD.1. The authentication mechanism supports authentication failure handling as addressed in FIA_AFL.1.</p> <p>User authentication via RMTs requires the use of a trusted path according to FTP_TRP.1.</p> <p>Authentication security management functions is implemented by FMT_SMF.1.</p>
O.Authorization	<p>User identification is addressed in FIA_UID.2. The requirement for access control is spelled out in FDP_ACC.1, and the access control policies are modeled in FDP_ACF.1. User-related attributes are spelled out in FIA_ATD.1.</p> <p>Access control is based on the definition of roles as subject and functions as object as defined in FMT_SMR.1 and FMT_MOF.1. Requirements on the management functionality for the definition of access control policies are provided in FMT_MSA.1/ACFATD, FMT_MSA.3/ACFATD.</p> <p>Authorization security management functions is provided in FMT_SMF.1.</p> <p>The requirements on management functionality for the definition of ACL are provided in FMT_MSA.1/IFF, FMT_MSA.3/IFF.</p>
O.Audit	<p>The generation of audit records is implemented by FAU_GEN.1. Audit records are supposed to include timestamp as provided by FPT_STM.1 and user identities as defined in FAU_GEN.2 where applicable.</p> <p>Requirements on reading audit records are defined in FAU_SAR.1. The protection of the stored audit records is implemented in FAU_STG.1. Functionality to delete the oldest audit file is provided if the size of the log files becomes larger than 100kB is required according to FAU_STG.3.</p> <p>The evidence to validate audit data is implemented by FDP_DAU.1.</p>

O.Integrity	<p>For tamper-proof protection of configuration data and audit logs is implemented by FDP_DAU1.3.</p> <p>For tamper-proof protection of Software version and firmware version is implemented by FDP_DAU2.1 and FCS_COP.1/RSA.</p>
O.Encryption	<p>The risk of information leakage is avoided by encrypting sensitive data (such as password, key) implementing in FCS_COP.1/PBKDF2, FCA_COP.1/AES and FCA_COP.1/SHA256.</p>
O.Communication	<p>Communication security is implemented by the establishment of a trusted path for remote users in FTP_TRP.1. Requirements on the security of the device authentication to establish a secure communication channel are defined in FDP_DAU.1.</p> <p>FCS_COP.1/AES, FCS_COP.1/SHA256, FCS_COP.1/SHA384, FCS_COP.1/RSA are providing the cryptographic functions required for TLS channels.</p> <p>FCS_COP.1/AES, FCS_COP.1/HMAC-SHA1, FCS_COP.1/HMAC-SHA2, FCS_COP.1/AES, FCS_CKM.1/DH are providing the cryptographic functions required for SSH/TLS channels.</p> <p>FCS_CKM.1/RSA and FCS_CKM.1/DH addresses key generation of AES/RSA keys. FCS_CKM.4 addresses key destruction of RSA keys. Note that keys of AES algorithms as a result of the DH key agreement are created and stored in a trunk of internal memory dynamically allocated within the TOE upon session establishment and are destroyed upon session termination according to FDP_RIP.1. The allocated memory is freed as well.</p> <p>Termination of a communication channel due to user inactivity is covered by FTA_SSL.3. Rejection of connections is addressed by FTA_TSE.1.</p>
O.SecurityManagement	<p>The management functionality for the security functions of the TOE is defined in FMT_SMF.1 and the security user roles are defined in FMT_SMR.1.</p>
O.AccessControl	<p>The requirement of ACL is defined in FDP_IFF.1 and FDP_IFC.1. The requirements on management functionality for the definition of ACL are provided in FMT_MSA.1/IFF, FMT_MSA.3/IFF.</p>

Table 8: SFR sufficiency analysis

5.4.3 Security Requirements Dependency Rationale

Dependencies within the EAL2 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

For the additional ALC_FLR.1 has no security requirement dependencies.

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

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
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_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH, Unsupported: FCS_CKM.4, substituted by FDP_RIP.1
FCS_COP.1/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/RSA FCS_CKM.4/RSA
FCS_COP.1/HMAC-SHA1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH , Unsupported: FCS_CKM.4, substituted by FDP_RIP.1

FCS_COP.1/HMAC-SHA2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/DH , Unsupported: FCS_CKM.4, substituted by FDP_RIP.1
FCS_COP.1/SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4
FCS_COP.1/SHA384	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4
FCS_COP.1/PBKDF2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/RSA FCS_CKM.4/RSA
FCS_CKM.1/DH	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/AES, FCS_COP.1/HMAC-SHA1, FCS_COP.1/HMAC-SHA2 Unsupported: FCS_CKM.4, substituted by FDP_RIP.1
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/RSA , FCS_CKM.4/RSA
FCS_CKM.4/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/RSA
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3/ACFATD
FDP_DAU.1	None	N/A
FDP_DAU.2	FIA_UID.1	N/A FIA_UID.2

FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1 FMT_MSA.3/IFF
FDP_RIP.1	None	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	N/A
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	None	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/ACFATD	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/IFF	[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/ACFATD	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1.1/ACFATD FMT_SMR.1
FMT_MSA.3/IFF	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1.1/IFF FMT_SMR.1
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FTA_SSL.3	None	N/A

FTA_TSE.1	None	N/A
FTP_TRP.1	None	N/A
FPT_STM.1	None	N/A

Table 9: Dependencies between TOE Security Functional Requirements

5.4.4 Justification for Unsupported Dependencies

The following dependencies are unsupported for the reasons given below.

FCS_COP.1/AES, FCS_COP.1/HMAC-SHA1, FCS_CKM.1/DH, FCS_COP.1/HMAC-SHA2: The dependency on FCS_CKM.4 (Key destruction) is unsupported, because the mechanism for destruction of symmetric keys is part of the session establishment but not a dedicated key destruction mechanism. Keys of AES/HMAC-SHA1/HMAC-SHA2 algorithms are created and stored in a trunk of internal memory dynamically allocated within the TOE upon session establishment and are destroyed upon session termination according to FDP_RIP.1. So FDP_RIP.1 acts as a substitute to the mechanism according to FCS_CKM.4 for these temporary session keys. Therefore the mechanism is not modeled as dedicated key destruction mechanism by FCS_CKM.4 although the objective of the SFR – the destruction of the key when no longer in use – is fulfilled.

FCS_COP.1/SHA256, FCS_COP.1/SHA384: Hash functions do not require keys, so FCS_CKM.1 and FCS_CKM.4 are not applicable.

5.5 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2+ALC_FLR.1 components. No operations are applied to the assurance components.

5.6 Security Assurance Requirements Rationale

The Evaluation Assurance Level 2+ALC_FLR.1 has been chosen to commensurate with the threat environment that is experienced by typical consumers of the TOE.

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

6.1 Authentication

The TOE can identify administrators by a unique ID and enforces their authentication before granting them access to any TSF management interfaces. Detailed functions include:

- 1) The TOE supports authentication via username and password. This function is achieved by comparing user information input with pre-defined reference values stored in memory.
- 2) The TOE stores the following security attributes for individual users:
 - User ID
 - User Level
 - SHA256 Hashes of Passwords(PBKDF2 algorithm)
 - Number of unsuccessful authentication attempts since last successful authentication
 - Time when users are logging in and logging off
- 3) The TOE mandates the use of a trusted path for user authentication according to 1) via Remote Management Terminals (RMTs).
- 4) The TOE supports the detection of 3 consecutive failed authentication attempts after the last successful user authentication, the termination of the secure channel required for authentication in that case and the blocking of the related user account for authentication for at least 5 minutes.
- 5) The TOE requires each user to be successfully authenticated before he can perform any other TSF-mediated actions except authentication according to 1) when connecting to the TOE.
- 6) The TOE requires each user to be successfully identified before he can perform any other TSF-mediated actions except authentication according to 1) when connecting to the TOE. The username is used for identification of the user.

(FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FTP_TRP.1, FMT_SMF.1)

6.2 Authorization

The TOE enforces an access control by supporting following functions:

- Support seven user groups.
- Support assigning a user group to each account.
- Accounts are managed in groups. There are seven user groups, including Super administrator, Read-only, Device administrator, Firmware administrator, Scope administrator, File transfer operator, Alarm reporting operator. Super administrator, Read-only, Device administrator, Firmware administrator, Scope administrator roles can be managed by WebUI. Alarm reporting operator, File transfer operator roles are not display on the WebUI. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account is used to attempt any unauthorized operation, an error message is displayed and the attempt is logged. The authority of each user group is specified in the following table.

User roles/Group	Authority	Security function
Super administrator	The accounts of this group are used for security management and are authorized to perform all query and configuration operations and assign a user to a different user role.	Authentication Authorization Auditing Communication Security Access Control Cryptographic functions Security Management Software Integrity Protection
Read-only	The accounts of this group have read-only permission for all resources.	Authentication Authorization Auditing Access Control Security Management
Device administrator	This account has server, E9000 management authority, mainly including server status and alarm query, server configuration, firmware upgrade and OS deployment functions.	Authentication Authorization Auditing Access Control Security Management
Firmware administrator	The accounts of this group have server firmware upgrade related permissions.	Authentication Authorization Auditing Access Control Security Management

User roles/Group	Authority	Security function
Scope administrator	The accounts of this group have the relevant permissions of domain operation, read permissions of all resources.	Authentication Authorization Auditing Access Control
File transfer operator	The accounts of this group have permission to transfer files.	Authorization Auditing Access Control
Alarm reporting operator	The accounts of this group have permission to receive BMC alarm events.	Authorization Auditing Access Control

(FDP_ACC.1, FIA_ATD.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1)

6.3 Auditing

The TOE can provide auditing ability by receiving all types of logs and processing them according to user's configuration:

- 1) The TOE supports generation of audit records for the following events:
 - i. user activity
 - User login and logout
 - ii. Management of user accounts
 - Add, delete, modify (refers to account authority))
 - Password change (by the user himself or administrator)
 - User Locking and Unlocking
 - User role change
 - Security Policy Configuration
 - iii. Management of scope
 - Add, delete, modify
 - iv. Security policy modification
 - v. Certificate management
 - vi. System management
 - Operation requests (i.e. configuration of the device, FusionDirector update, firmware update, OS image deployment)
 - vii. Log management
 - log policy modification
- 2) The TOE records within each audit record the date and time of the event, type of event, subject identity (of applicable) and the outcome (success or failure) of the event. The TOE provides reliable time stamps for that purpose. Depending on the definition of the event records might include the interface, workstation IP, User ID or CLI command name.
- 3) The TOE supports association of audit events resulting from actions of identified users with the identity of the user that caused the event.

- 4) The TOE allows all authorized users (i.e. all authenticated users who have assigned a user level high enough to execute the commands for reading audit records) to read the audit records.
- 5) The TOE supports log file formats binary and readable text. This function is achieved by providing output format transformation. By this the TOE provides the user with audit information suitable for interpretation.
- 6) The TOE writes audit event information to the NVRAM first (buffer). The TOE supports local storage of audit event information in the internal data base, and output of audit event information to external audit servers.
- 7) The TOE does not support modification of audit information.
- 8) The TOE restricts the ability to delete audit event information to authorized users (i.e. all authenticated users who have assigned a user level high enough to execute the commands for deleting audit records).
- 9) Audit functionality is activated by default but can be deactivated by users with sufficient access rights. Logging of the event of disabling audit functionality is enforced by default.

(FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FAU_STG.3, FPT_STM.1, FDP_DAU.1)

6.4 Communication Security

The TOE provides communication security by the following mechanisms:

- 1) The TOE provides mechanisms to establish a trusted path between itself and a RMT based on the HTTPS or the SSH2.0 protocol (SSH is sometimes also referred to STelnet). In addition, SFTP (i.e. FTP based on SSH protocol) is supported for file transfer. The HTTPS and SSH protocol uses the cryptographic algorithms as specified in chap. 6.7 , item 9) and item 11).
- 2) The TOE permits remote users to initiate communication with the TOE to establish the trusted path.
- 3) The TOE supports mechanisms to verify the validity of the authentication information of SSH and can generate evidence about that which can be verified by SSH. For client user authentication the TOE supports password authentication according to chap. 9.4.5 [RFC 4251] and chap. 8 [RFC 4252], respectively. Server authentication is performed using RSA according to chap. 6.6 [RFC 4253], ssh-rsa.
- 4) The TOE supports mechanisms to verify the validity of the authentication information of HTTPS and can generate evidence about that which can be verified by HTTPS. For client user authentication the TOE supports password authentication according to chap. 7.4.6 [RFC 4346] and [RFC 5246]. Server authentication is performed using RSA according to chap. 7.4.2 [RFC 4346] and [RFC 5246].
- 5) The TOE supports termination of an interactive session after a given interval of user inactivity.
- 6) The TOE makes temporary session keys stored in volatile memory inaccessible upon termination of SSH sessions.
- 7) The TOE provides NTP client function to synchronize time from NTP server. The TOE also provides NTP server function to synchronize time with server BMC. The NTP client connect a NTP server using standard NTP protocol. The TOE provides auditing ability.

- 8) The TOE provides NFS server functionality for downloading OS image files. To control access, the TOE provides IP whitelist function. The TOE also provides auditing ability.

(FDP_DAU.1, FDP_RIP.1, FTA_SSL.3, FTA_TSE.1, FTP_TRP.1, FPT_STM.1, FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA1, FCS_COP.1/HMAC-SHA2, FCS_CKM.1/DH, FCS_CKM.1/RSA)

6.5 Access Control

The TOE enforces an access control by supporting following functionalities:

- 1) The TOE supports the association of user roles with user IDs, each user role assigns the corresponding operational privileges. The TOE manages user privileges by user roles. There are seven user roles by default, each user role has different permissions. A user can access a command if the access rights of the command match those of the user role.
- 2) The TOE requires each user to be successfully identified before he can perform any other TSF-mediated actions except authentication according to Authentication when connecting to the TOE. The username is used for identification and the user level of the user is used for access control.
- 3) The TOE protects equipment from network attacks by controlling data of access requests from unauthorized IP addresses and ports. The TOE refuses to receive and process messages from the blacklist by configuring the URL blacklist and can limits the frequency of external IP requests.

(FDP_ACC.1, FDP_ACF.1, FIA_UID.2, FMT_MOF.1, FMT_MSA.1/ACFATD, FMT_MSA.1/ IFF, FMT_MSA.3/ACFATD, FMT_MSA.3/IFF, FMT_SMR.1, FDP_IFC.1, FDP_IFF.1)

6.6 Security Management

The TOE offers management functionality for its security functions. Security management functionality can either be used through Web-based Console.

The access control mechanisms of the TOE are based on user role's permission control. Each user role assigns the corresponding permission. Only the operation with the corresponding permission of user role can be executed.

Modifications have to be saved, otherwise they will be lost after reboot of the TOE. The TOE loads the saved device configuration during start-up, so saved modifications are not lost by rebooting the device. After reset to factory defaults, the TOE is in the factory configuration.

The security management functionality comprises:

- User management
 - User Rights configuration
 - Scope configuration
 - Two-factor authentication configuration
- Account policy management
 - Maximum number of accounts created by the system

- Lockout Period After Consecutive Login Failures
- Account Name Minimum, Maximum Length Limit
- Password policy management
 - Historical Password Reuse Limit
 - Account Locked Due to Incorrect Password Attempts
 - Minimum Change Interval
 - Validity Period
 - Weak Password Dictionary
- Session policy management
 - Session timeout
 - System Creation Session Upper Limit
- Certificate management, mainly certificate updating
 - 1) The TOE supports the configuration of the interval for user inactivity after that an established session is terminated;
 - 2) The TOE supports the configuration of System Creation Session Upper Limit;
 - 3) The TOE supports the configuration of User management
 - User Rights configuration
 - Scope configuration
 - Two-factor authentication configuration
 - 4) The TOE supports the configuration of Account policy management
 - Maximum number of accounts created by the system
 - Lockout Period After Consecutive Login Failures
 - Account Name Minimum, Maximum Length Limit
 - 5) The TOE supports the configuration of Password policy management
 - Historical Password Reuse Limit
 - Account Locked Due to Incorrect Password Attempts
 - Minimum Change Interval
 - Validity Period
 - Weak Password Dictionary
 - 6) The TOE supports the configuration of Session policy management
 - Session timeout
 - System Creation Session Upper Limit
 - 7) The TOE supports Certificate management, mainly certificate updating;

- 8) The TOE supports the management of user accounts (creating, maintaining, and deleting user accounts) and user data (username, password including password reset). The TOE supports the assignment of user roles to users and the maintenance of these user roles;
- 9) The TOE supports the configuration of the output channel for audit log (e.g. output to external syslog servers).

(FMT_SMF.1, FDP_DAU.1)

6.7 Cryptographic Functions

Cryptographic functions are required by security features as dependencies. The following cryptographic algorithms are supported:

- 1) The TOE supports symmetric encryption and decryption using the AES algorithm in CBC mode according to [FIPS 197] and [FIPS SP 800-38A] using key lengths of 128bits. AES-128 CBC is used for encryption and decryption within SSH communication.
- 2) The TOE supports asymmetric authentication of the TOE (server) to the client using the RSA algorithm according to [PKCS#1 V2.1], RSASSA-PKCS1-v1_5 using a key length of 2048bits. RSA with key size of 3072bits according to PKCS#1 V2.1, RSASSA-PKCS1-v1_5 together with SHA256 is used for asymmetric authentication for SSH according to chap. 6.6 [RFC 4253], SSH-RSA.
- 3) The TOE supports data integrity generation and verification using the HMAC-SHA1 algorithm according to [RFC 2104], [FIPS 198-1] using key lengths of 160 bits. The data integrity protection mechanism is used for integrity protection for SSH communication.
- 4) The TOE supports hashing of data using SHA256 algorithm according to [FIPS 180-4].
- 5) The TOE supports generation of cryptographic keys according to diffie-hellman-group14-sha1 and specified cryptographic key sizes 2048bits according to [RFC 4253], [RFC 3526], [PKCS#3] for SSH. The TOE generates a shared secret value with the client during the DH key agreement. The shared secret value is used to derive session keys used for encryption and decryption (AES-128-CBC) and generation and verification of integrity protection information (HMAC-SHA1) for SSH communication. The key generation is performed according to [RFC 4253], chap. 7.2.
- 6) The TOE supports key generation for the RSA algorithm according to [FIPS 186-4] using CRT. RSA keys generated have a key length of 2048bits and are intended for usage with RSASSA-PKCS1-V1_5.
- 7) The TOE supports the destruction of RSA keys by overwriting them with 0.
- 8) The TOE can use the deterministic random number generator provided by Go language. The generator corresponds to the requirements of class DRG.2 according to [AIS20]. The random numbers are used for generation of 128bit AES keys, RSA keys of 2048bits, 3072bits and 160bit HMAC keys.
- 9) The TOE supports the SSH protocol according to [RFC 4251], [RFC 4252], [RFC 4253], [RFC 4254] and the following cipher suites according to [RFC 4253]:
 - Diffie-hellman-group14-sha1 or diffie-hellman-group1-sha256 as key exchange algorithm of SSH.
 - AES-128-CTR encryption and decryption algorithm.
 - RSA (3072 bits) according to [PKCS#1 V2.1], RSASSA-PKCS1-V1_5 for asymmetric authentication of the TOE (server) to the client.

- HMAC-SHA1, HMAC-SHA2-256 or HMAC-SHA2-512 data integrity generation and verification algorithm.
- 10) The TOE supports the HTTPS (TLS1.2/1.3) protocol according to [RFC 4346] and [RFC 5246], and the following cipher suites according to [RFC 8492]:
- ECDHE, DHE, RSA as key exchange algorithm of HTTPS.
 - AES-128/256 (GCM or CBC mode) encryption and decryption algorithm.
 - RSA (2048 bits) according to [PKCS#1 V2.1], RSASSA-PKCS1-V1_5 for asymmetric authentication of the TOE (server) to the client.
 - HMAC-SHA1, HMAC-SHA2-256 or HMAC-SHA2-384 data integrity generation and verification algorithm.

(FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/HMAC-SHA1, FCS_COP.1/HMAC-SHA2, FCS_COP.1/SHA256, FCS_COP.1/SHA384, FCS_COP.1/PBKDF2, FCS_CKM.1/DH, FCS_CKM.1/RSA, FCS_CKM.4/RSA)

6.8 Software Integrity Protection (Digital Signature)

The TOE provides the ability to verify software validity and prevent the installation of insecure or unauthorized software. FusionDirector uses the digital signature mechanism to protect the software package integrity.

All software versions which are released and ready for production are signed by development before the transfer to production. Software versions are unique. The versions of the released software images and related documents must match the software versions. By verifying the signature and the version information and checking against the version information used for certification of a product, the certified version can be identified. The TOE provides:

- a) FusionDirector release packages support the OpenPGP digital signature function. The process is as follows:
- When a FusionDirector release version is built, an OpenPGP digital signature is created by interacting with the xFusion digital signature center. The software package and the digital signature file are released together on the xFusion support website.
 - The xFusion digital signature center releases the OpenPGP digital signature verification tool and public key on the xFusion support website.
 - During version update, obtain the software version, digital signature file, digital signature verification tool, and public key from the xFusion support website (<https://support.xFusion.com/carrier/digitalSignatureAction>), and use the digital signature tool and public key to verify the digital signature of the software version.
 - ◆ If the verification is successful, continue to load the software.
 - ◆ If the verification fails, stop loading the software.
- b) The integrity of firmware packages on FusionDirector is checked by using the crypto message syntax (CMS) mechanism. The process is as follows:
- When a FusionDirector firmware version is built, a CMS digital signature is created by interacting with the xFusion digital signature center. The software package and the digital signature file are released together on the xFusion support website.
 - FusionDirector supports the CMS verification function and the public key.

- When updating firmware, obtain the firmware package and the digital signature file from the xFusion support website.
- The verification process is performed by FusionDirector and does not require manual intervention.
 - ◆ If the verification is successful, continue to load the firmware.
 - ◆ If the verification fails, stop loading the firmware.

(FDP_DAU.2, FCS_COP.1/RSA)

7 Abbreviations, Terminology and References

7.1 Abbreviations

ACL	Access Control List
AES	Advanced Encryption Standard
CC	Common Criteria
CLI	Command Line Interface
LMT	Local Maintenance Terminal
NTP	Network Time Protocol
RMT	Remote Maintenance Terminal
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
RSA	Rivest Shamir Adleman
SFTP	Secure File Transfer Protocol
SSH	Secure Shell
TLS	Transport Layer Security
O&M	Operations and Maintenance
IAM	Identity and Access Management
MQ	Message Queue
LDAP	Lightweight Directory Access Protocol
RBAC	Role-based access control
RMT	Remote Management Terminal

CMS	Crypto Message Syntax
LMT	Local Management Terminal
VXLAN	Virtual eXtensible Local Area Network
SPC	System Patch Cold
BMC	Baseboard Management Controller
IRM	Intelligent Rack Management
ETH	Interface Ethernet
NFVI	Network Function Virtualization Infrastructure

7.2 Terminology

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

<i>Administrator</i>	An administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE’s point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE. Since all user levels are assigned to commands and users and users can only execute a command if their associated level is equal or higher compared to the level assigned to a command, a user might have certain administrative privileges but lacking some other administrative privileges. So the decision whether a user is also an administrator or not might change with the context (e.g. might be able to change audit settings but cannot perform user management).
<i>Operator</i>	See User.
<i>User</i>	A user is a human or a product/application using the TOE which is able to authenticate successfully to the TOE. A user is therefore different to a subject which is just sending traffic through the device without any authentication.
<i>E9000</i>	E9000 is a 12U chassis server. It can house 8 full-width compute nodes or 16 half-width compute nodes.
<i>BMC</i>	BMC is an out of band management system optimized for server remote management of compute node.
<i>scope</i>	The resources of a system can be divided into different scopes based on the actual requirements. When creating a user, it can be specified the scope.
<i>public network</i>	Public network refers to the communication network built by network service providers for

	public users. The communication lines of the public network are shared for public users.
<i>business network</i>	Business network refers to the communication network used to transfer customer's transaction data.
<i>management network</i>	Management network refers to the communication network used to monitor, configure, analyze and control software and hardware resources.

7.3 References

- [CC] Common Criteria for Information Technology Security Evaluation, Part 1-3, Version 3.1 Revision 5, April 2017
- [FIPS 197] Federal Information Processing Standards Publication 197, November 26, 2001
- [FIPS 198-1] Federal Information Processing Standards Publication 198-1, July 2008
- [FIPS 180-4] Federal Information Processing Standards Publication 180-4, August 2015
- [FIPS 186-4] Federal Information Processing Standards Publication 186-4, July 2013
- [PKCS #1] PKCS #1 v2.1: RSA Cryptography Standard, June 14, 2002
- [PKCS #5] Password-Based Cryptography Specification Version 2.0, September 2000
- [NIST] NIST Special Publication 800-56A Revision 3, April 2018
- FusionDirector Installation Guide 01, April 16 2022
- [NIST SP 800-57] NIST Special Publication 800-57 Rev. 2 – Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, March 2019
- [PKCS#3] PKCS #3: Diffie-Hellman Key- Agreement Standard, version 1.4, November 1993
- [RFC 2104] RFC 2104 - HMAC: Keyed-Hashing for Message Authentication, February 1997
- [RFC 2437] PKCS #1: RSA Cryptography Specifications Version 2.0, October 1998
- [RFC 2898] PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000
- [RFC 3174] RFC 3174 - US Secure Hash Algorithm 1 (SHA1), September 2001
- [RFC 3268] RFC 3268 - Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002
- [RFC 3526] RFC 3526 - More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003
- [RFC 4250] RFC 4250 - The Secure Shell (SSH) Protocol Assigned Numbers, January 2006
- [RFC 4251] RFC 4251 - The Secure Shell (SSH) Protocol Architecture, January 2006

- [RFC 4252] RFC 4252 - The Secure Shell (SSH) Authentication Protocol, January 2006
- [RFC 4253] RFC 4253 - The Secure Shell (SSH) Transport Layer Protocol, January 2006
- [RFC 4254] RFC 4254 - The Secure Shell (SSH) Connection Protocol, January 2006
- [RFC 4346] RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1, April 2006
- [RFC 4492] RFC 4346 - Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), May 2006
- [RFC 4634] RFC 4634 - US Secure Hash Algorithms (SHA and HMAC-SHA), July 2006
- [RFC 5246] RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2, August 2008
- [RFC 5288] RFC 5288 - AES Galois Counter Mode (GCM) Cipher Suites for TLS, August 2008
- [RFC 8017] RFC 8017 - PKCS #1: RSA Cryptography Specifications Version 2.2, November 2016
- [RFC 8492] RFC 8492 - Secure Password Ciphersuites for Transport Layer Security (TLS), February 2019