Common Criteria Certification
Security Target v1.0

Adtran
FSP 3000R7 Operating System (EAL2)
Rel. 22.1.3

Classification: - Public -

(C) 2024 Adva Network Security GmbH. All rights reserved.

CC ST FSP 3000R7 OS (EAL2) Rel. 22.1.3

Classification: - ***Public*** -

Document owner: Nadine Fritz

Document Polarion number: STAR-2093

Document type: Common Criteria (CC) Certification Security Target (ST)

Document version: 1.0

Revision date: N/A

Revision editor: Nadine Fritz

Status: ✔ Published

Table 1: Version history

Version	Date	Remark	Editor
1.0	2024-02-21	Document creation	Nadine Fritz

Table of contents

(C) 2024 Adva Network Security GmbH. All rights reserved.

(C) 2024 Adva Network Security GmbH. All rights reserved.

(C) 2024 Adva Network Security GmbH. All rights reserved.

List of figures

(C) 2024 Adva Network Security GmbH. All rights reserved.

List of tables

(C) 2024 Adva Network Security GmbH. All rights reserved.

1 Security Target introduction (C)

This chapter presents ST and TOE identification information, summarizes the ST in narrative form and provides information for a potential user to determine whether the Fiber Service Platform (FSP) 3000R7 network element is of interest. An ST contains the security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements.

An ST principally defines:

a. A security problem expressed as a set of assumptions about the security aspects of the operational environment, a list of threats that the TOE is intended to counter, and any known rules with which the TOE must comply. See chapter 3.
b. A set of security objectives and a set of security requirements to address the security problem. See chapters 4 and 6.
c. The security functionality provided by the TOE that meets the requirements. See chapter 7.

Document specifics:

The document covers the common (core) elements of the security solution of a product line and the specifics of one individual TOE. It is referenced in section 1.1 Security Target and TOE references (I). The core elements are indicated with "(C)", and appear in the Security Targets for different TOEs. The individual product elements are indicated with "(I)".
Additionally, the document includes icons to facilitate a quick visual recognition of items related to each other. For an overview of the icons and its definitions, see the Appendix.

1.1 Security Target and TOE references (I)

Table 2: Security Target reference

Title:	Common Criteria Certification Security Target Adtran FSP 3000R7 Operating System Release 22.1.3
Short Title:	CC ST Adtran FSP 3000R7 Operating System
Version:	1.0
Date:	February 20th, 2024
Authors:	Nadine Fritz Paweł Tyszkowski
Security Target prepared by:	Adva Network Security GmbH Hermann-Dorner-Allee 91 12489 Berlin, Germany
Security Target prepared for:	Adtran Networks SE Campus Martinsried Fraunhoferstraße 9a 82152 Martinsried/Munich Germany

Table 3: TOE reference

TOE name:	Adtran FSP 3000R7 Operating System Release 22.1.3 and its related guidance documentation
TOE short name:	Adtran FSP 3000R7 Operating System
TOE version:	Release 22.1.3
TOE developer:	Adtran, Inc.
CC identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 ([CC])
Evaluation Assurance Level:	EAL2
PP conformance:	none

(C) 2024 Adva Network Security GmbH. All rights reserved.

1.2 TOE overview

The TOE overview summarizes the usage and major security features of the TOE. The TOE overview provides a context for the TOE evaluation by describing the product and defining the specific evaluated configuration.

1.2.1 Introduction (C)

The FSP 3000R7 is a scalable optical transport solution designed to respond to today's exploding bandwidth demands. It can be used by service providers or in an enterprise environment. The modular design of the FSP 3000R7 ensures that networks are built on a flexible WDM1 foundation. The FSP 3000R7 represents Optical and Ethernet provisioning for seamless end-to-end connectivity from the access to the metro and on to long haul.

Figure 1: FSP 3000R7 family

The TOE consists of the operating system of the NCU (NCU-II or NCU-3). The hardware (mainboard, casing, interface modules) is not in the scope of the evaluation unless addressed by any assumption relating the operational environment. For descriptions of the TOE security functionalities, see chapter 7 TOE summary specification (C).

All TOE components as well as the intended operational environment of the TOE are illustrated in this figure.

(C) 2024 Adva Network Security GmbH. All rights reserved.

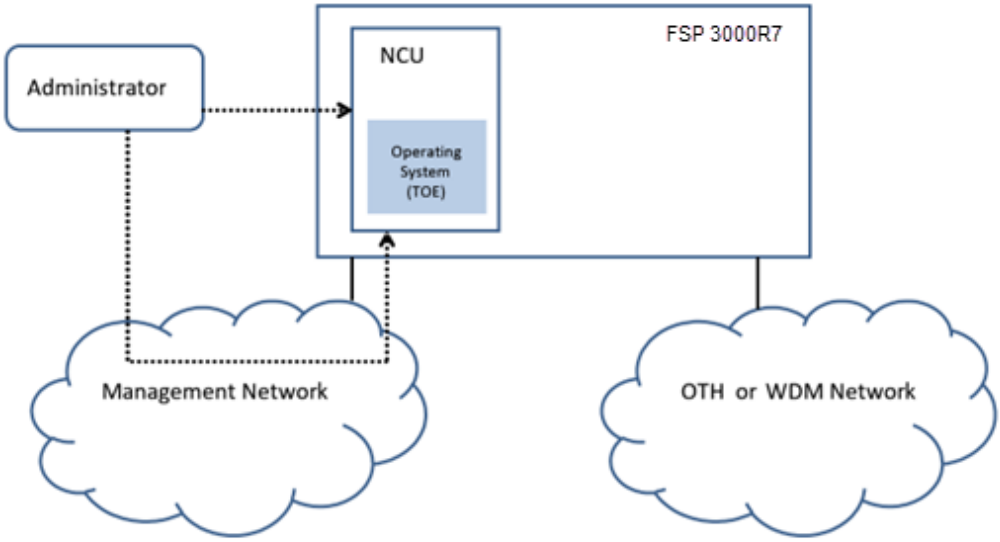


Figure 2: TOE boundary

1.2.2 Brief description of the TOE components

The TOE is the operating system of the FSP 3000R7 system that can be found in the NCU-II card (see Figure 3*)* or NCU-3 *(*see Figure 4*)*.

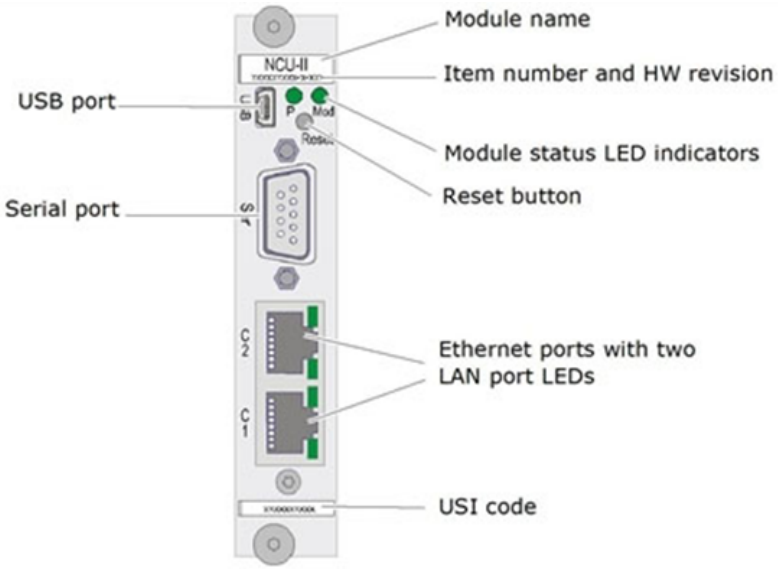


Figure 3: NCU-II card

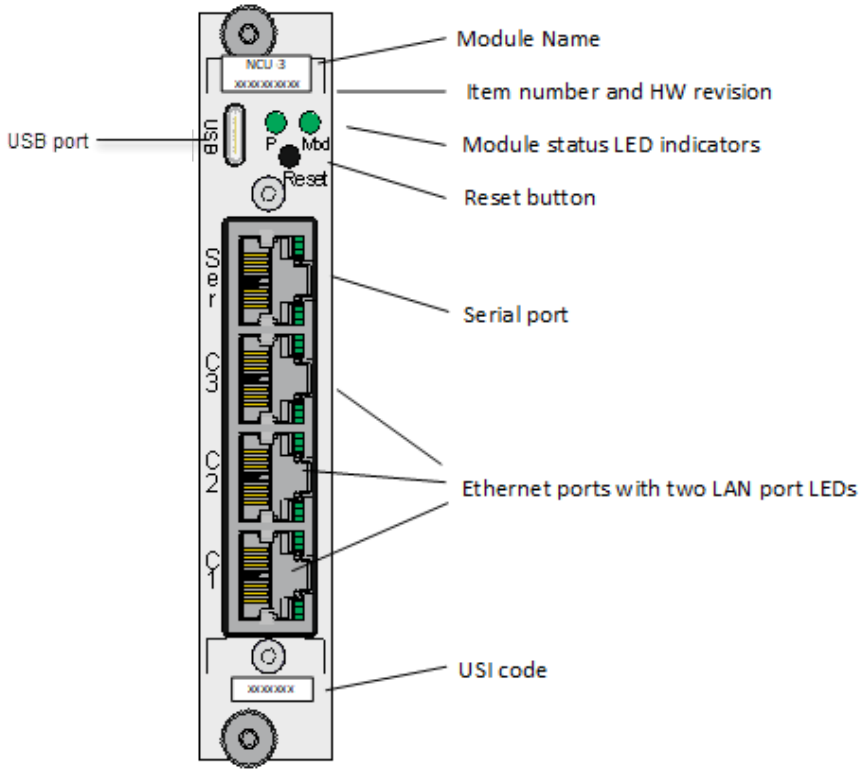


Figure 4: NCU-3 card

The NCU-II and NCU-3 are network element control (NCU) units providing system management capabilities and network connection to the FSP 3000R7 system. They are single-slot, 2.5 HU high plug-in modules and acts as the hardware interface between the different modules of the system and the equipment connected to the NCU's management interfaces.

The external connectors of the NCU-II include two RJ45 Ethernet ports, one serial USB and one serial DE9M interface.

The external connectors of the NCU-3 include three RJ45 Ethernet ports, one serial USB and one serial RJ45 interface.

The NCU-II and NCU-3 can be accessed through a serial, USB or Ethernet port. The NCU-II and NCU-3 must be configured for the specific operating environment. Depending on the capabilities of the network element, specific Right to Use (RTU) versions may be required.

The evaluated version of the operating system supports local using serial/USB connection and remote connections using SSH, HTTPS or SNMPv3 protocol at the Ethernet port of the NCU-II or NCU-3. The connection is encrypted to ensure confidentiality, integrity and authenticity of the transferred data. Serial and USB connections have not been evaluated and are outside the scope of the certified usage.

The Ethernet ports labeled C1 and C2 (and C3 NCU-3) are female 8P8C (RJ-45) receptacles and can be

(C) 2024 Adva Network Security GmbH. All rights reserved.

used to connect the NCU-II or NCU-3 to a network management system or a management PC, either directly or via an external network, using standard Ethernet crossover cabling.

Table 4: TOE reference

Component	Type	TOE Reference
NCU-II or NCU-3	Hardware	Not under evaluation of the TOE.
NCU-II or NCU-3 Serial Port	Hardware	Not under evaluation of the TOE.
NCU-II or NCU-3 Serial Port	Hardware	Not under evaluation of the TOE.
Operation System of NCU-II or NCU-3	Software	TOE

The TOE can be downloaded from the Adtran Networks SE customer portal web. The software in a zip file format is part of a complete FSP 3000R7 system software identified by the release number.

The software and user guides for FSP 3000R7 can be loaded from the **https://advaoptical.my.salesforce.com** web page as registered customer.

1.2.3 Brief description of the TOE operational environment

Only one NCU is supported per network element. One NCU is able to manage a complete network element. The NCU must be installed in the master shelf and requires a shelf control unit (SCU) in each (master + any additional) shelf to communicate with the modules. The NCU-3 requires a shelf control unit of type SCU-II.
An NCU communicates with the SCU types in the master shelf using an internal system bus. Exchange of information between the SCU types in the master shelf and the SCU types in the additional shelves takes place over the management fiber ring.
Over the management network an administrative remote connection to the TOE (NCU-II or NCU-3 operating system) can be established. In the following we always speak of NCU which means either NCU-II or NCU-3.

An overview of the TOE and the immediate operational environment is provided in Figure 5 and Figure 6.

Key elements of the TOE operational environment are:

- 19” – mountable shelf versions
- A central Network Element Controller unit (NCU) which can handle up to 25 shelves via a single IP address
- A shelf controller (SCU)
- Channel Cards for 2.5Gbit/s, 4Gbit/s, 10Gbit/s or 100Gbit/s support all relevant Telco or Datacom

(C) 2024 Adva Network Security GmbH. All rights reserved.

protocols.

- Erbium Doped Fiber (EDFA) and Raman amplifiers
- Various types of WDM filters supporting up to 96 different ITU-T compliant wavelengths
- Reconfigurable Optical Add Drop Modules (ROADM)
- Protection switch modules
- Optical supervisory Channel Modules (OSCM)

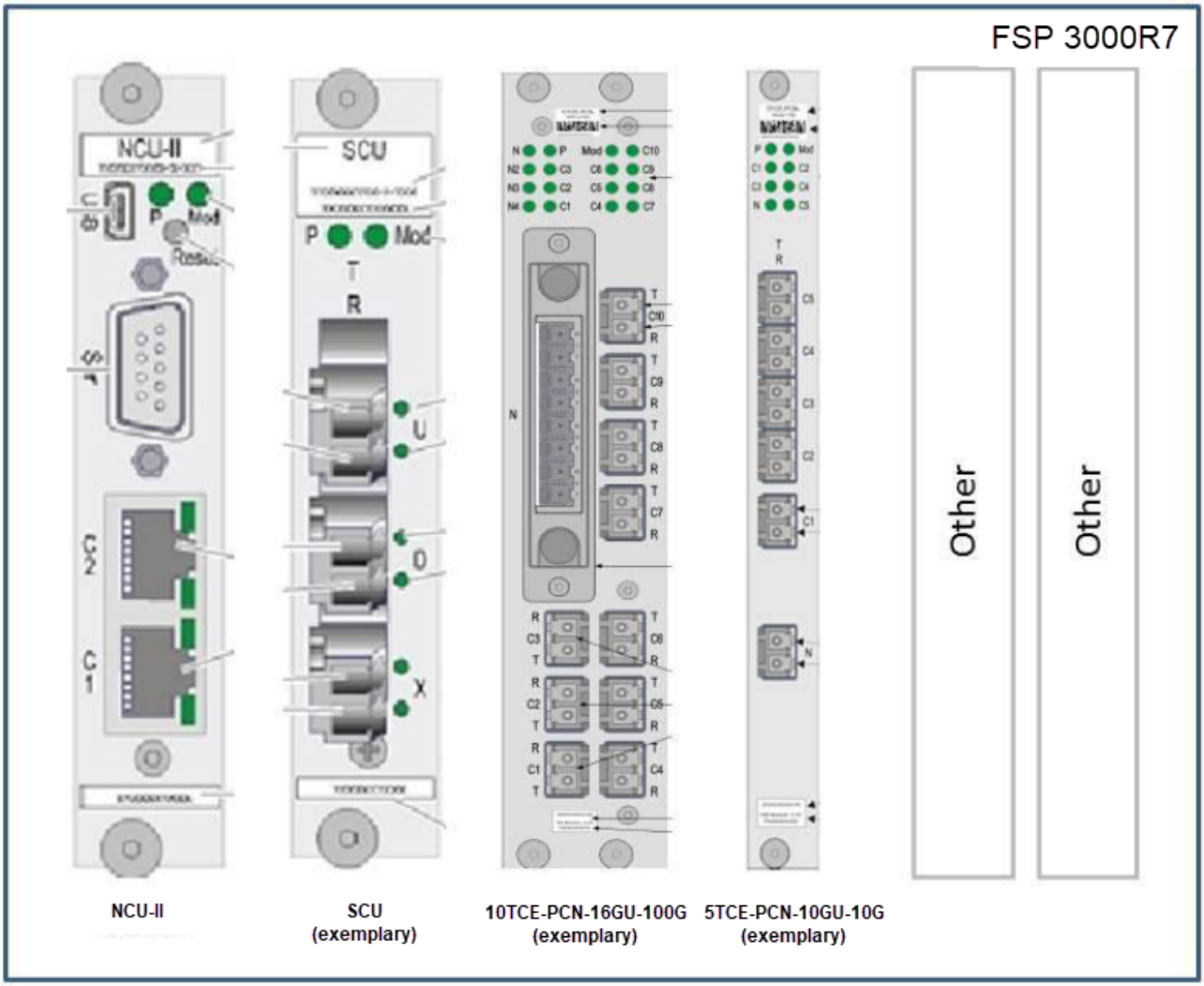


Figure 5: NCU-II card in its operational environment

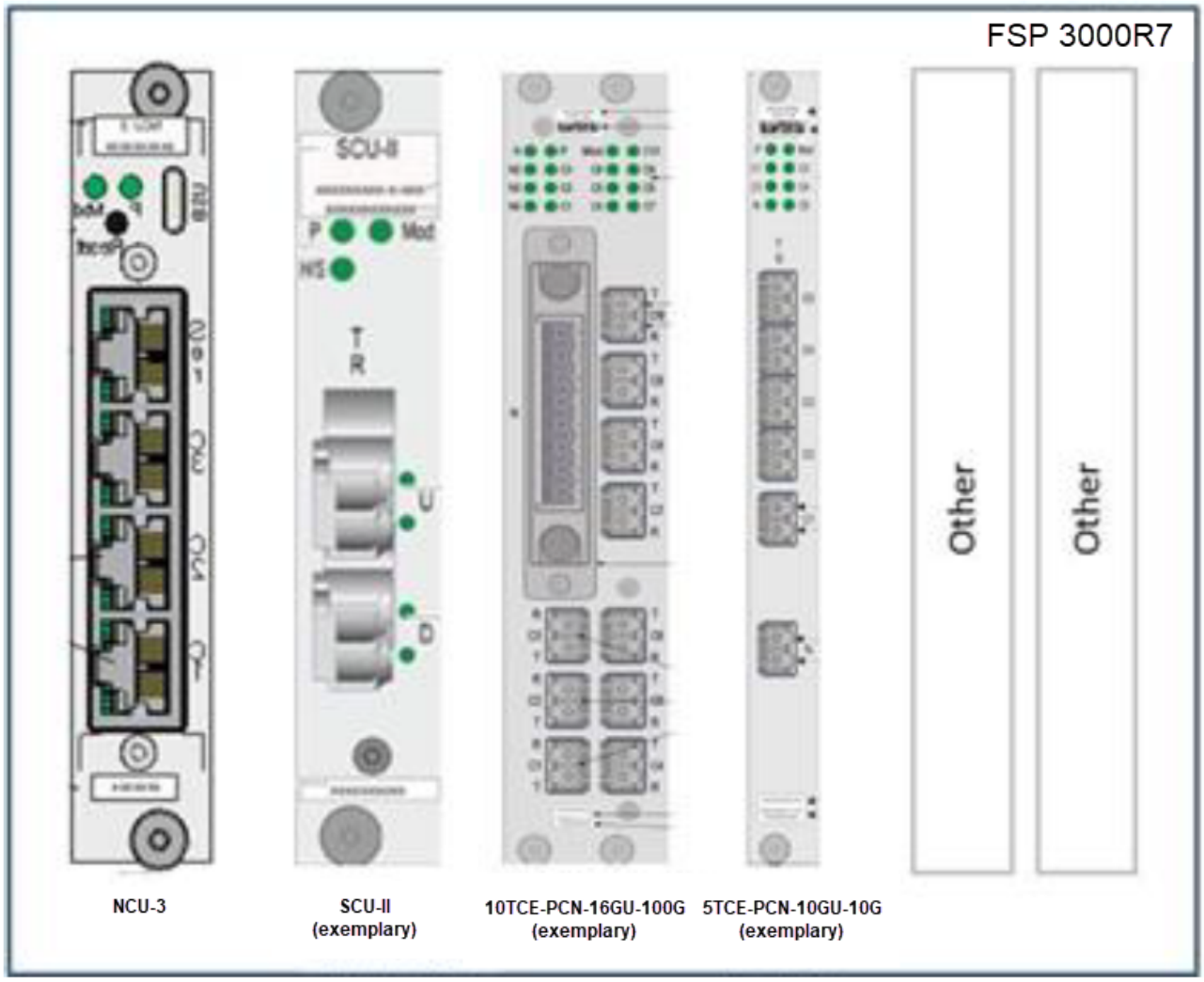


Figure 6: NCU-3 card in its operational environment

1.3 TOE description

The product Fiber Service Platform (FSP) 3000R7 is a transport platform for fiber optic applications. Key technologies of the product are Wavelength Division Multiplexing (WDM), optical amplification, wavelength switching, time division multiplexing as well as Ethernet aggregation. The system takes client protocols like Ethernet, SDH, or Fiber Channel and maps them into the ITU-T G.709 transport protocol hierarchy along with an optical conversion from a standard 850nm or 1310nm optical port on the client side of the system to an ITU-T – compliant WDM wavelength on the network side of the system. The system is completely modular.

The next subsections describe the physical scope and logical scope of the TOE.

(C) 2024 Adva Network Security GmbH. All rights reserved.

1.3.1 TOE physical scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the operational environment of the TOE. The TOE is a software only product. The TOE component is an NCU with its FSP 3000R7 operating system. The evaluated NCU operating system is of FSP 3000R7 Rel. 22.1.3.

The TOE does not have any further hard- or software requirements, since it is provided as a stand-alone solution that does not allow any user modifications except configuration.

1.3.1.1 User documentation (I)

For the release 22.1.3 of the NCU with its FSP 3000R7 operating system, guidance for users is given in these user manuals. Additional references are provided in the Release Notes R22.1.3 (document no 890 00002227-11).

Table 5: Overview of the NCU with its FSP 3000R7 operating system user manuals rel. 22.1.3

Manual name	Document number	File name	Includes security-related sections
Hardware Description	80000073284	FSP3000R7_R22.1_Hardware_ Description_IssA.pdf	yes
High-Density Subshelf Hardware Guide	80000073293	FSP3000R7_R22.1_High-Density_Subshelf_Guide_ IssA.pdf	
Installation and Commission-ing Manual	80000073282	FSP3000R7_R22.1_Installation_and_ Commissioning_ Manual_ IssA.pdf	
Maintenance and Troubleshoot-ing Manual	80000073283	FSP3000R7_R22.1_Maintenance_ and_Troubleshooting_ Manual_ IssA.pdf	
Management Data Guide	80000073287	FSP3000R7_R22.1_Management_ Data_ Guide_IssA.zip	
Module and System Specification	80000073290	FSP3000R7_R22.1_Module_System_ Specification_ IssA.pdf	

(C) 2024 Adva Network Security GmbH. All rights reserved.

NETCONF User Guide	80000073292	FSP3000R7_R22.1_NETCONF_User_ Guide_ IssA.pdf	yes
Network Element Director Online Help	80000073254	FSP3000R7_R22.1_Network_Element_ Director_Help_ IssA.pdf	yes
Provisioning and Operations Manual	80000073280	FSP3000R7_R22.1_Provisioning_and _Operations_ Manual_ IssA.pdf	yes
Safety Guide	80000073289	FSP3000R7_R22.1_Safety Guide_IssA.pdf	yes
Secure System Configuration Guide	80000073294	FSP3000R7_R22.1_Secure_ System_Configuration_Guide_ IssA.pdf	yes

For details about the manuals that include security-related sections, see the related Assurance Guidance Documents (AGD).

1.3.2 TOE logical scope (I)

The logical boundary of the TOE is divided into the following security classes which are described in detail within chapter 7. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Functionality:

- Protected Communication
- System Monitoring
- TOE Administration
- TSF Self Test

(C) 2024 Adva Network Security GmbH. All rights reserved.

1.3.2.1 Protected communications

To ensure that sensitive data is transmitted to and from the TOE the TOE will provide encryption for these trusted paths between themselves and the endpoint. These channels are implemented using following standard protocols:

- HTTPS (TLS), and
- SSH, and
- SNMPv3.

These protocols are specified by RFCs that offer a variety of implementation choices. Requirements have been imposed on some of these choices (particularly those for cryptographic primitives) to provide interoperability and resistance to potential attacks.
The SSH, TLS, and SNMPv3 are used to established the secure administration path. These channels provide the confidentiality and integrity security measures of the transmitted data. The end points are authenticated what makes the man-in-the-middle attack infeasible.

1.3.2.2 System monitoring

In order to assure that information exists that allows administrators to discover intentional and unintentional issues with the configuration and/or operation of the system, the TOEs have the capability of generating audit data targeted at detecting such activity. Auditing of administrative activities provides information that may hasten corrective actions should the system be configured incorrectly. Audit of selected system events can provide an indication of failure of critical portions of the TOE (e.g., repeated failures to establish sessions, or authenticate to the system) of a suspicious nature.

1.3.2.3 TOE administration

In order to provide a trusted means for administrators to interact with the TOE, the TOE provides a password-based logon mechanism. The administrator has the capability to compose a strong password. To avoid attacks where an attacker might observe a password being typed by an administrator, passwords must be obscured during logon. Session locking or termination must also be implemented to mitigate the risk of an account being used illegitimately. Passwords must be stored in an unreadable form, and there must be no interface provided for specifically reading the password or password file such that the passwords are displayed in plain text.

(C) 2024 Adva Network Security GmbH. All rights reserved.

1.3.2.4 TSF self test

In order to detect failures of underlying security mechanisms used by the TSF, the TSF will perform self-tests.

1.4 Conventions

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [italicized text within brackets].
- Completed selection statements are identified using [underlined text within brackets].

Refinements are identified using bold text. Any text removed is stricken (Example: TSF Data) and should be considered as a refinement.
Extended Functional and Assurance Requirements are identified using “_EXT” at the end of the short name.

Iterations are identified by appending a number in parentheses following the component title. For example**, FAU_GEN.1 (1) Audit Data Generation** would be the first iteration and **FAU_GEN.1 (2) Audit Data Generation** would be the second iteration.

(C) 2024 Adva Network Security GmbH. All rights reserved.

2 Conformance claims (C)

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. This chapter contains the following sections:

- CC conformance claims
- PP claim
- Package claim
- Conformance rational

2.1 CC conformance claim (C)

This Security Target claims to be conform to the Common Criteria 3.1:

- Part 2 extended to [CC]: In order to provide a complete description of the functional requirements addressed by the TOE, functional components of part 2 of the Common Criteria framework were used. But also additions to the Common Criteria part 2 were defined, to fulfill the requirement of a complete and consistent TOE description.
- Part 3 conform to [CC]: For the description of the requirements due to the trustworthiness of the TOE, only security assurance requirements of CC part 3 where used.

2.2 PP claim

This ST does not claim conformance to any PP.

2.3 Package claim

This Security Target claims to be conform to the Security Assurance Requirements package EAL 2.

2.4 Conformance rationale

Though the ST does not claim conformance to any PP it borrows several aspects from the [CPP-ND].

(C) 2024 Adva Network Security GmbH. All rights reserved.

3 Security problem definition

This section describes the security aspects of the TOE and the operational environment in which the TOE will be used or is expected to be employed. The security aspects include:

- Assets the TOE must protect.
- Threat agents interacting with the TOE.
- Threats existing against those TOE assets.
- Organizational security policies the TOE shall comply with.
- Assumptions made on the operational environment to provide security functionality when using the TOE.

3.1 Assets (C)

All assets the TOE is to protect are listed as follows:

Asset	Description
TSF data	Data for the operation of the TOE upon which the enforcement of the SFR relies. It contains TOE configuration and audit records.
TOE executable code	The TOE software.
User data	Data on management plane that is transferred by the TOE (FSP 3000R7 Operating System (CC)) either plain or encrypted.

3.2 Threat agents

All threat agents interacting with the TOE are listed as follows:

Threat agent	Description
ATTACKER_OR_MALICIOUS_USER	An entity who is attempting to subvert the operation of the TOE. The intention may be to gain unauthorized access to the assets protected by the TOE. They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and has no physical access to the TOE.
SECURITY_ADMINISTRATOR	An authenticated user who has unrestricted access to the TOE and is able to manage the TOE functionality. Administrators are responsible for the management of all TOE processes and have to ensure that the TOE operates in a secure way. Especially only Administrators are allowed to modify the configuration.

(C) 2024 Adva Network Security GmbH. All rights reserved.

IT_ENTITY	An IT entity sending data to or receiving data from the TOE.

3.3 Threats

All threats against which the TOE must protect the assets are listed as follows:

T.PASSWORD_CRACKING: A malicious user may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.

T.SECURITY_FUNCTIONALITY_COMPROMISE: A malicious user may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.

T.SECURITY_FUNCTIONALITY_FAILURE: A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS: A malicious user may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

T.UNDETECTED_ACTIVITY: A malicious user may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.

T.UNTRUSTED_COMMUNICATION_CHANNELS: A malicious user may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the middle attacks, replay attacks, etc.
Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

T.WEAK_AUTHENTICATION_ENDPOINTS: A malicious user may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into

(C) 2024 Adva Network Security GmbH. All rights reserved.

the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

3.4 Organizational security policies (C)

An organizational security policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The OSPs are listed as follows:

P.ACCESS_BANNER: The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

3.5 Assumptions (C)

The following specific conditions are required to ensure the TOE security and are assumed to exist in an environment where this TOE is employed.
The assumptions for the TOE security environment are defined as follows:

A.ADMIN_CREDENTIALS_SECURE: The administrator credentials (e.g. passwords) used to access the TOE are protected by the platform on which they reside.

A.LIMITED_FUNCTIONALITY: The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking functionality).

A.NO_THRU_TRAFFIC_PROTECTION: A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it.
The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ST.

A.PHYSICAL_PROTECTION: The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the ST will not include any requirements on physical tamper protection or other physical attack mitigations. The ST will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.

A.TRUSTED_ADMINISTRATOR: The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device.

(C) 2024 Adva Network Security GmbH. All rights reserved.

The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

(C) 2024 Adva Network Security GmbH. All rights reserved.

4 Security objectives (C)

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see chapter 3). The security objectives form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security objectives for the TOE (C)

The TOE security objectives are defined as follows:

O.DISPLAY_BANNER: The TOE will display an advisory warning regarding use of the TOE.

O.PROTECTED_COMMUNICATIONS: The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

O.SESSION_LOCK: The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.

O.SYSTEM_MONITORING: The TOE will provide the capability to generate and store audit data. So compromise credentials and device data enabling continued access to the network device and its critical data, failures during start-up or during operations, unauthorized administrator access to the network device, and access, change, and/or modify the security functionality can be recognized.

O.TOE_ADMINISTRATION: The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE. It ensures that administrators use strong passwords and it also provides protections for logged-in administrators. The TOE will also provide secure protocols to authenticate the endpoints.

O.TSF_SELF_TEST: The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

4.2 Security objectives for the operational environment (C)

The security objectives for the operational environment are based on the secure usage of the assumptions and are defined as follows:

OE.ADMIN_CREDENTIALS_SECURE: The administrator credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.NO_GENERAL_PURPOSE: There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE environment, other than those services necessary for the operation, administration, and support of the TOE.

OE.NO_THRU_TRAFFIC_PROTECTION: The TOE does not provide any protection of traffic that

(C) 2024 Adva Network Security GmbH. All rights reserved.

traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.TRUSTED_ADMIN: TOE administrators are trusted to follow and apply all guidance documentation in a trusted manner.

4.3 Security objectives rationale (C)

4.3.1 Overview

Table 6: Security objectives rationale overview

Organizational security policy (OSP), threats and assumptions vs. security objectives	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATION	O.SESSION_LOCK	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	OE.NO_GENERAL_PURPOSE	OE.ADMIN_CREDENTIALS_SECURE	O.TSF_SELF_TEST	OE.NO_THRU_TRAFFIC_PROTECTION	OE.PHYSICAL	OE.TRUSTED_ADMIN
P.ACCESS_BANNER	X						-	-	-	-	-
T.PASSWORD_CRACKING					X		-	-	-	-	-
T.SECURITY_FUNCTIONALITY_ COMPROMISE				X	X		-	-	-	-	-
T.SECURITY_FUNCTIONALITY_ FAILURE				X		X	-	-	-	-	-
T.UNAUTHORIZED_ ADMINISTRATOR_ACCESS			X	X	X		-	-	-	-	-
T.UNDETECTED_ACTIVITY				X			-	-	-	-	-
T.UNTRUSTED_COMMUNICATION_CHANNELS		X					-	-	-	-	-

T.WEAK_AUTHENTICATION_ENDPOINTS					X		-	-	-	-	-
A.ADMIN_CREDENTIALS_SECURE	-	-	-	-	-	-	X				
A.NO_GENERAL_PURPOSE	-	-	-	-	-	-		X			
A.NO_THRU_TRAFFIC_ PROTECTION	-	-	-	-	-	-			X		
A.PHYSICAL_PROTECTION	-	-	-	-	-	-				X	
A.TRUSTED_ADMINISTRATOR	-	-	-	-	-	-					X

4.3.2 Enforcing the organizational security policies

P.ACCESS_BANNER is enforced by **O.DISPLAY_BANNER** since it ensures that the TOE displays an advisory warning before any identification action is performed.

Every identified organizational security policy is countered by one or more security objectives

4.3.3 Countering the threats (C)

Every identified organizational security policy is countered by one or more security objectives
T.PASSWORD_CRACKING is countered by **O.TOE_ADMINISTRATION** since this TOE security objective provides mechanisms to ensure that administrators do not use weak passwords.

T.SECURITY_FUNCTIONALITY_COMPROMISE is countered by

- **O.TOE_ADMINISTRATION** since this TOE security objective provides mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
- **O.SYSTEM_MONITORING** since it ensures that the TOE provides the capability to generate audit data of administrative actions.

T.SECURITY_FUNCTIONALITY_FAILURE is countered by

- **O.SYSTEM_MONITORING** since it ensures that the TOE provides the capability to generate audit data of TSF failures.
- **O.TSF_SELF_TEST** since it ensures that the TOE provides the capability to test some subset of its security functionality to ensure it is operating properly

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS is countered by

- **O.SESSION_LOCK** since this TOE security objective provides mechanisms that mitigate

(C) 2024 Adva Network Security GmbH. All rights reserved.

the risk of unattended sessions being hijacked.
- **O.SYSTEM_MONITORING** since it ensures that the TOE provides the capability to generate audit data of administrative actions like logon trials.
- **O.TOE_ADMINISTRATION** since this TOE security objective provides mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.

T.UNDETECTED_ACTIVITY is countered by **O.SYSTEM_MONITORING** since it ensures that the TOE provides the capability to generate audit data of administrative actions.

T.UNTRUSTED_COMMUNICATION_CHANNELS is countered by **O.PROTECTED_COMMUNICATIONS** since this TOE security objective provides protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

T.WEAK_AUTHENTICATION_ENDPOINTS is countered by **O.TOE_ADMINISTRATION** since this TOE security objective provides mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.

Every identified threat is countered by one or more security objectives.

4.3.4 Upholding the assumptions (C)

A.NO_GENERAL_PURPOSE is upheld by **OE.NO_GENERAL_PURPOSE**, since it ensures that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

A.PHYSICAL_PROTECTION is upheld by **OE.PHYSICAL**, since it ensures physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

A.TRUSTED_ADMINISTRATOR is upheld by **OE.TRUSTED_ADMIN**, since it ensures that TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

A.ADMIN_CREDENTIALS_SECURE is upheld by **OE.ADMIN_CREDENTIALS_SECURE**, since it ensures that TOE Administrators credentials (private key) used to access TOE must be protected on any other platform on which they reside.

A.NO_THRU_TRAFFIC_PROTECTION is upheld by **OE.NO_THRU_TRAFFIC_PROTECTION**, since it ensures TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

Every assumption is upheld by one objectives for the operational environment. The justification above demonstrates that the defined security objectives for the operational environment uphold all defined assumptions.

(C) 2024 Adva Network Security GmbH. All rights reserved.

5 Extended components definition

This chapter defines TOE security functional requirements and assurance requirements which are not part of CC 3.1 part 2 or part 3.
The assurance requirements that have been defined by the Common Criteria v3.1 part 3 are applicable to the extended components.
Because this component is a software component with a well-defined behavior on its external interfaces, the assurance requirements that have been defined in part 3 of Common Criteria are applicable to this functional family.
Through its nature as a software component the assurance classes ADV, AGD, ALC, ATE and AVA are applicable in the evaluation process. It is not required to define a new assurance class or assurance family for a consistent and complete description to cover this SFR. This SFR does not define any behavior that might require an extension of part 3 of the Common Criteria Evaluation Framework.

5.1 Extended TOE Security functional components

This section specifies the extended SFRs for the TOE.

5.1.1 Class FCS: Cryptographic support

The existing FCS functionality class was extended because part II of [CC] does not contain any SFR, which defines following functionalities:

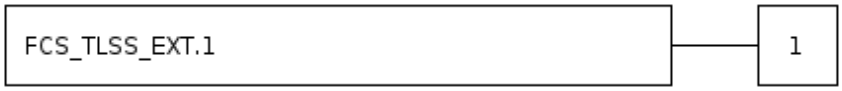
- defining the explicit usage of the TLS sever protocol,
- defining the explicit usage of the SSH protocol,
- defining the explicit usage of the HTTPS protocol.

5.1.1.1 TLSS Protocol (FCS_TLSS_EXT1)

CC - FCS_TLSS_EXT.1 Explicit: TLS

This section describes the extended SFRs for TLS Server Protocol (FCS_TLSS_EXT):

- Family Behavior: This family defines the requirements for explicit TLS usage.
- Component leveling:



FCS_TLSS_EXT defines the usage of an explicit TLS server protocol.

- Management: **FCS_TLSS_EXT.1**
  There are no management activities foreseen.

- Audit: **FCS_TLSS_EXT.1**
  The following actions should be auditable if **FAU_GEN** Security audit data generation is included in the PP/ST:
  - Minimal: Failure to establish a TLS session.
  - Minimal: Establishment/Termination of a TLS session.

Hierarchical to: No other component
Dependencies: **FCS_CKM.1** Cryptographic key generation, **FCS_CKM.4** Cryptographic key destruction

FCS_TLSS_EXT.1.1 - The TSF shall implement [**TLS 1.2** (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289]

and no other cipher suites.

FCS_TLSS_EXT.1.2 - The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [TLS 1.1].

FCS_TLSS_EXT.1.3 - The TSF shall perform key establishment for TLS using: [

- RSA with key size [3072 bits, 4096 bits],
- Diffie-Hellman parameters with size [3072 bits],
- ECDHE curves [secp256r1, secp384r1, secp521r1] and no other curves

].

FCS_TLSS_EXT.1.4 - The TSF shall support [no session resumption or session tickets].

Application Note: Many TLS settings are configurable, f.e. an administrator may disable unwanted ciphersuits.

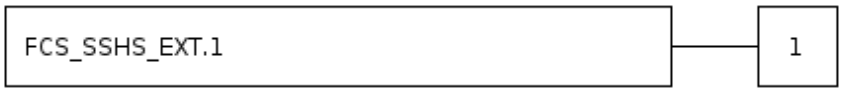
(C) 2024 Adva Network Security GmbH. All rights reserved.

5.1.1.2 SSH Protocol (FCS_SSHS_EXT)

CC - FCS_SSHS_EXT Explicit: SSH

This section describes the extended SFRs for FCS_SSHS_EXT:

- Family Behavior: This family defines the requirements for explicit SSH usage.
- Component leveling



FCS_SSHS_EXT.1 defines the usage of an explicit SSH protocol.

- Management: **FCS_SSHS_EXT.1**
  There are no management activities foreseen.
- Audit: **FCS_SSHS_EXT.1**:
  The following actions should be auditable if **FAU_GEN** Security audit data generation is included in the PP/ST:
  - Minimal: Failure to establish a SSH session.
  - Minimal: Establishment/Termination of a SSH session.

Hierarchical to: No other components.
Dependencies: **FCS_CKM.1** Cryptographic key generation, **FCS_CKM.4** Cryptographic key destruction

FCS_SSHS_EXT.1.1 - The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [5647, 5656, 8268].

FCS_SSHS_EXT.1.2 - The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [password-based].

FCS_SSHS_EXT.1.3 - The TSF shall ensure that, as described in RFC 4253, packets greater than [*32,768*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 - The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CTR-128, AES-CTR-192, AES-CTR-256, [AEAD_AES_256_GCM] and rejects all other encryption algorithms.

FCS_SSHS_EXT.1.5 - The TSF shall ensure that the SSH public-key based authentication implementation uses [rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 - The TSF shall ensure that the SSH transport implementation uses [hmac-

(C) 2024 Adva Network Security GmbH. All rights reserved.

sha2-256, hmac-sha2-512, AEAD_AES_256_GCM, implicit] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 - The TSF shall ensure that [diffie-hellman-group15-sha512, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512] and [ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521], no other methods] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 - The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

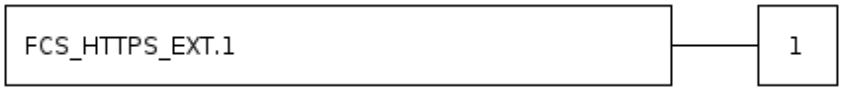
Application Note: Many SSH settings are configurable, f.e. an administrator may disable unwanted ciphers.

5.1.1.3 HTTPS Protocol (FCS_HTTPS_EXT)

CC - FCS_HTTPS_EXT Explicit: HTTPS

This section describes the extended SFRs for FCS_HTTPS_EXT:

- Family Behavior: This family defines the requirements for explicit HTTPS usage.
- Component leveling:



FCS_HTTPS_EXT.1 defines the usage of an explicit HTTPS protocol.

- Management: **FCS_HTTPS_EXT.1**
  There are no management activities foreseen.
- Audit: **FCS_HTTPS_EXT.1**
  The following actions should be auditable if **FAU_GEN** Security audit data generation is included in the PP/ST:
  - Minimal: Failure to establish a HTTPS session.
  - Minimal: Establishment/Termination of a HTTPS session.

Hierarchical to: No other components
Dependencies: FCS_TLSS_EXT.1

FCS_HTTPS_EXT.1.1 - The TSF shall implement the HTTPS protocol that complies with RFC 2818.

(C) 2024 Adva Network Security GmbH. All rights reserved.

FCS_HTTPS_EXT.1.2 - The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1

5.1.2 Class FIA: Identification and authentication

CC - Class FIA: Identification and authentication

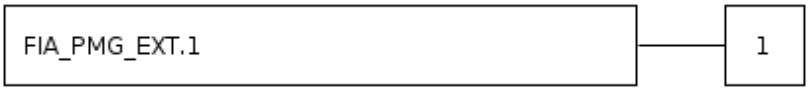
The existing FIA functionality class was extended because part II of [CC] does not contain any SFR which defines the complexity of password mechanism.

5.1.2.1 Password management (FIA_PMG_EXT)

CC - FIA_PMG_EXT

This section describes the extended SFRs for FIA_PMG_EXT:

- Family Behavior: This family defines the requirements for password management.
- Component leveling:



- Management: **FIA_PMG_EXT.1**
  Configuration of the password complexity may be considered for the management functions in FMT.
- Audit: **FIA_PMG_EXT.1**: There are no auditable events foreseen.

Hierarchical to: No other components
Dependencies: No dependencies

FIA_PMG_EXT.1.1 - The TSF shall provide the following password management capabilities for administrative passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “(”, “)”, [“_” , “+” , “|” , “~” , “{”, “ }” , “[” , “]” , “-”, “.”]];
- Minimum password length shall be configurable to between [15] and [128] characters.

Application Note:

"Administrative passwords" refers to passwords used by administrators at the local console, over protocols that support passwords, such as SSH, HTTPS and SNMPv3.
We recommend enabling Security Enhanced Mode which enforce at least 15 password characters and the password change for all currently created accounts.

(C) 2024 Adva Network Security GmbH. All rights reserved.

5.1.3 Class FPT: Protection of the TSF

CC - Class FPT: Protection of the TSF

The existing FPT functionality class was extended because part II of [CC] does not contain any SFR, which defines following functionality:

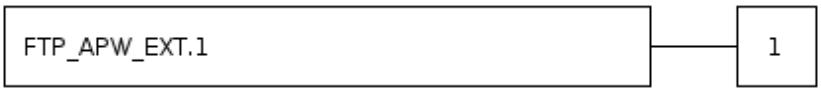
- protection of administrator passwords,
- testing of TOE security functionality.

5.1.3.1 Protection of Administrator passwords (FPT_APW_EXT)

CC - FPT_APW_EXT

This section describes the extended SFRs for FPT_APW_EXT:

- Family Behavior: This family defines the requirements for the protection of administrator passwords.
- Component leveling



FPT_APW_EXT.1 Protection of Administrator Passwords, defines how the TSF shall store passwords.

- Management: **FPT_APW_EXT.1**: There are no management activities foreseen.
- Audit: **FPT_APW_EXT.1**: There are no auditable events foreseen.

Hierarchical to: No other components
Dependencies: No dependencies

FPT_APW_EXT.1.1 - The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 - The TSF shall prevent the reading of plaintext passwords.

Application Note: The intent of the requirement is that raw password authentication data are not stored in the clear, and that no user or administrator is able to read the plain text password through “normal” interfaces. An all-powerful administrator of course could directly read memory to capture a password but is trusted not to do so.

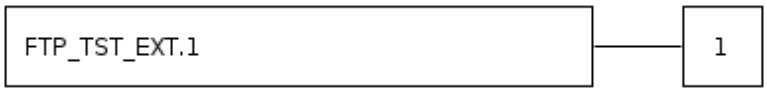
(C) 2024 Adva Network Security GmbH. All rights reserved.

5.1.3.2 TSF testing – Extended (FPT_TST_EXT)

CC - TSF testing – Extended (FPT_TST_EXT)

This section describes the extended SFRs for FPT_TST_EXT:

- Family Behavior: This family defines the requirements for the testing TOE security functionality.
- Component leveling



FPT_TST_EXT.1.1 - The TSF shall run a suite of the following self-tests [during initial start-up (on power on)] to demonstrate the correct operation of the TSF: [*software integrity, file system integrity*]. NCU-II checks file system integrity. NCU-3 checks software integrity and file system integrity.

- Management: **FPT_TST_EXT.1**: The following actions could be considered for the management functions in FMT:
  - management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions;
  - management of the time interval if appropriate.
- Audit: **FPT_TST_EXT.1**: The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
  - Basic: Execution of the TSF self tests and the results of the tests.

Hierarchical to: No other components.
Dependencies: No dependencies.

Application Note:

- The TOE itself checks essential supporting functionality (File system and Database) that is required for a flawless operation of the TSF on demand of an authorized user via the management software.
- The software integrity checks use SHA-384 digests to validate software executable files and libraries.

(C) 2024 Adva Network Security GmbH. All rights reserved.

5.2 Extended TOE security assurance components

There are no extended TOE security assurance components.

(C) 2024 Adva Network Security GmbH. All rights reserved.

6 Security requirements

CC - Security requirements

This chapter defines the security requirements that shall be satisfied by the TOE or its operational environment:
Common Criteria divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g. configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the next subchapters.

6.1 Security functional requirements

CC - Security functional requirements

The specified functional requirements are compliant with Common Criteria v3.1 part 2 and are corresponding with the given functional components.

Table 7: TOE Security functional requirements

Name	Description
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FCS_CKM.1	Cryptographic key generation (for asymmetric keys)
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1(1)	Cryptographic operation (for data encryption/decryption)
FCS_COP.1(2)	Cryptographic operation (for cryptographic signature)
FCS_COP.1(3)	Cryptographic operation (for cryptographic hashing)
FCS_COP.1(4)	Cryptographic operation (for keyed-hash message authentication)
FCS_TLSS_EXT.1	Explicit: TLS Server without mutual authentication
FCS_SSHS_EXT.1	Explicit: SSH
FCS_HTTPS_EXT.1	Explicit: HTTPS

(C) 2024 Adva Network Security GmbH. All rights reserved.

FIA_PMG_EXT.1	Password management
FIA_UID.1	Timing of identification
FIA_UAU.2	User authentication before any action
FIA_UAU.7	Protected authentication feedback
FMT_MTD.1	Management of TSF Data (for general TSF data)
FMT_SMF.1	Specification of management functions
FMT_SMR.2	Restrictions on security roles
FPT_APW_EXT.1	Protection of administrator passwords
FPT_STM_EXT.1	Reliable Time Stamps
FPT_TST_EXT.1	TSF Testing - extended
FTA_SSL.3	TSF-initiated termination
FTA_SSL.4	User-initiated termination
FTA_TAB.1	Default TOE access banners
FTP_TRP.1	Trusted path

6.1.1 Class FAU – Security audit

CC - FAU_GEN.1 Audit data generation

This section describes the SFRs for FAU_GEN.1 Audit Data Generation:

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

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

- Start-up and shut-down of the audit functions;
- All auditable events, for the [not specified] level of audit; and
- [*All administrative actions comprising:*

  - *Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).*
  - *Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*

- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*

- *Specifically defined auditable events listed in Table 8: Auditable Events].*

FAU_GEN.1.2 - The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
- For each audit event type, based on the auditable event definitions of the functional components included in the ST, [*information specified in column three of Table 8: Auditable Events]*.

Table 8: Auditable events

Requirement	Auditable event (s)	Additional audit record contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_TLSS_EXT.1	Failure to establish a TLS session.	Reason for failure.
FIA_PMG_EXT.1	None.	None.
FIA_UAU.7	None.	None.
FIA_UAU.2	All use of the identification and	Origin of the attempt (e.g., IP address).

(C) 2024 Adva Network Security GmbH. All rights reserved.

	authentication mechanism.	
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failures of the trusted path functions.	Identification of the claimed user identity.

Application note: A shutdown information is never logged since the TOE is not intended to be shut down.

CC - FAU_GEN.2 User identity association

This section describes the SFRs for FAU_GEN.2 User identity association:

- Hierarchical to: No other components.
- Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 - Timing of identification

FAU_GEN.2.1 - For audit events resulting from actions of identified users, the TSF shall be able to

(C) 2024 Adva Network Security GmbH. All rights reserved.

associate each auditable event with the identity of the user that caused the event.

6.1.2 Class FCS – Cryptographic support

CC - Class FCS – Cryptographic support

The following tables contain the CAVP algorithm certificates for the cryptographic library implemented in the TOE:

Table 9: Cryptographic algorithm

SFR	Algorithm/Protocol	OpenSSL CAVP cert #
FCS_CKM.1	ECC schemes per FIPS PUB 186-4	CAVP Certificate #A4284
	FFC using safe-prime groups per NIST Special Publication 800-56A Revision 3 and RFC 3526.	-
FCS_CKM.2	Elliptic curve-based key establishment per NIST Special Publication 800-56A Revision 3	CAVP Certificate #A4284
	FFC using safe-prime per NIST Special Publication 800-56A Revision 3 and groups listed in RFC 3526.	-
FCS_COP.1/DataEncryption	AES CTR 256 bits, AES GCM 256 bits per following FIPS PUB 197	CAVP Certificate #A4284
FCS_COP.1/SigGen	ECDSA signature schemes per FIPS PUB 186-4	CAVP Certificate #A4284
	RSA signature schemes per FIPS PUB 186-4	-
FCS_COP.1/Hash	SHA digest schemes per FIPS Pub 180-4 Secure Hash Standard (SHS)	CAVP Certificate #A4284
FCS_COP.1/KeyedHash	Keyed hash scheme HMAC-384 per FIPS PUB 180-4	CAVP Certificate #A4284
	Keyed hash scheme HMAC-256 per FIPS PUB 180-4	-

The OpenSSL CAVP certificates are based on the FSP 3000R7 Operating System Release 22.2.2, but the cryptographic algorithms and their implementations are the same for Release 22.1.3.

CC - FCS_CKM.1 Cryptographic key generation (for asymmetric keys)

This section describes the SFRs for FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys):

(C) 2024 Adva Network Security GmbH. All rights reserved.

Hierarchical to: No other components.
Dependencies:

- FCS_COP.1 Cryptographic operation
- FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 - The TSF shall generate cryptographic asymmetric keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes that meet the following standards:

Table 10: Cryptographic key generation algorithm

Usage	Cryptographic key generation algorithm	Key size	Standards
SSH	DH	key strength of at least 3072 bits	FFC schemes using cryptographic key sizes of 3072-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1
	ECDH		ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4
HTTPS	DH	key strength of at least 3072 bits	FFC schemes using cryptographic key sizes of 3072-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1
	ECDH		ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4
	RSA		RSA schemes using cryptographic key sizes of 3072-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3
TLS	DH	key strength of at least 3072 bits	FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1
	ECDH		ECC schemes using “NIST curves” [P-256, P-384, P-521]

(C) 2024 Adva Network Security GmbH. All rights reserved.

			that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4
	RSA		RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3

CC - FCS_CKM.2 Cryptographic key establishment

This section describes the SFRs for FCS_CKM.2 Cryptographic key establishment:

Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.2.1 - The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;
- FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [groups listed in RFC 3526].

].

CC - FCS_CKM.4 Cryptographic key destruction

This section describes the SFRs for FCS_CKM.4 Cryptographic key destruction:

Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 - The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroize*] that meets the following: [*none*].

Application Note: The TSF shall zeroize all plaintext secret and private cryptographic keys when the keys are no longer required.

CC - FCS_COP.1(1) Cryptographic operation (for data encryption/decryption)

This section describes the SFRs for FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption):

Hierarchical to: No other components.

(C) 2024 Adva Network Security GmbH. All rights reserved.

Dependencies:

- FCS_CKM.1 Cryptographic key generation,
- FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1) - The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES operating in GCM, [CTR]*] and cryptographic key sizes [*128 bits, 192 bits, 256 bits*], that meets the following: [*FIPS PUB 197, "Advanced Encryption Standard (AES)", NIST SP 800-38A, NIST SP 800-38D*].

CC - FCS_COP.1(2) Cryptographic operation (for cryptographic signature)

This section describes the SFRs for FCS_COP.1(2) Cryptographic Operation (for cryptographic signature):
Hierarchical to: No other components.
Dependencies:

- FCS_CKM.1 Cryptographic key generation,
- FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(2) - The TSF shall perform *cryptographic signature services* in accordance with a specified cryptographic algorithm and cryptographic key sizes that meet the following standards:

Table 11: Cryptographic signature services

Cryptographic signature	Key size	Standards
RSA Digital Signature Algorithm	key size (modulus) of 3072 bits or greater	FIPS PUB 186-4, "Digital Signature Standard"
ECDSA Digital Signature Algorithm	256 bits or greater	FIPS PUB 186-4, "Digital Signature Standard"

Application Note: RSA and ECDSA algorithms are used for signing the self-signed X.509 certificates, also realizing key exchange for TLS and SSH protocols.

CC - FCS_COP.1(3) Cryptographic operation (for cryptographic hashing)

This section describes the SFRs for FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing):

Hierarchical to: No other components.
Dependencies:

- FCS_CKM.1 Cryptographic key generation,
- FCS_CKM.4 Cryptographic key destruction

(C) 2024 Adva Network Security GmbH. All rights reserved.

FCS_COP.1.1(3) - The TSF shall perform [*cryptographic hashing services* in accordance with a specified cryptographic algorithm and message **hash** sizes that meet the following standards:

Table 12: Cryptographic hashing services

Operations	Hash algorithms	Standards
HTTPS	SHA-256, SHA-384	FIPS PUB 180-4
	AES-GCM	supported additionally
SSH	HMAC SHA-256, HMAC SHA-512	FIPS PUB 180-4
	AEAD_AES_256_GCM	supported additionally
SNMPv3	HMAC-SHA256, HMAC-SHA512	RFC 2104 (HMAC)

Application Note: The TOE also supports AES-GCM which is not part of FIPS PUB 180-3.

CC - FCS_COP.1(4) Cryptographic operation (for keyed-hash message authentication)

This section describes the SFRs FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication):

Hierarchical to: No other components.
Dependencies:

- FCS_CKM.1 Cryptographic key generation,
- FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(4) - The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm and message hash sizes that meet the following standards:

Table 13: Keyed-hash message authentication

Operations	Hash algorithms / hash sizes	Standards
keyed-hash message authentication	HMAC SHA-256, HMAC SHA-512	FIPS PUB 180-4

CC - FCS_TLSS_EXT.1 Explicit: TLS

See section 5.1 Extended TOE Security functional component for details.

CC - FCS_SSH_EXT.1 Explicit: SSH

See section 5.1 Extended TOE Security functional component for details.

(C) 2024 Adva Network Security GmbH. All rights reserved.

CC - FCS_HTTPS_EXT.1 Explicit: HTTPS

See section 5.1 Extended TOE Security functional component for details.

6.1.3 Class FIA – Identification and authentication

CC - FIA_PMG_EXT.1 Password management

See section 5.1 Extended TOE Security functional component for details.

CC - FIA_UID.1 Timing of identification

This section describes the SFRs FIA_UID.1 Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 - The TSF shall allow [

- *Display the warning banner in accordance with FTA_TAB.1*

] on behalf of the user to be performed before the user is identified.

FIA_UID_1.2 - The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Application Note: The TSF shall display warning banner before the user is identified and then authenticated by FIA_UAU.2.

CC - FIA_UAU.2 User authentication before any action

This section describes the SFRs FIA_UAU.2 User authentication before any action:

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 - The TSF shall require each **Security Administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **Security Administrator**.

Application Note: The TSF shall provide a local password and key based authentication mechanisms to perform administrative user authentication.

CC - FIA_UAU.7 Protected authentication feedback

This section describes the SFRs FIA_UAU.7 Protected Authentication Feedback:

Hierarchical to: No other components.

(C) 2024 Adva Network Security GmbH. All rights reserved.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 - The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress **at the local console**.

Application Note: “Obscured feedback” implies the TSF does not produce a visible display of any authentication data entered by a user (such as the echoing of a password), although an obscured indication of progress may be provided (such as an asterisk for each character). It also implies that the TSF does not return any information during the authentication process to the user that may provide any indication of the authentication data.

6.1.4 Class FMT – Security Management

CC - FMT_MTD.1 Management of TSF data

This section describes the SFRs FMT_MTD.1 Management of TSF Data (for general TSF data):

Hierarchical to: No other components.
Dependencies:

- FMT_SMF.1 Specification of management functions
- FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to [*manage*] the [*the stored account information*] to [*the Security Administrators*].

Application Note:

> The word “manage” includes but is not limited to create, initialize, view, change default, modify, delete, clear, and append. This SFR includes also the resetting of user passwords by the Security Administrator.

CC - FMT_SMF.1 Specification of management functions

This section describes the SFRs FMT_SMF.1 Specification of Management Functions:

Hierarchical to: No other components.
Dependencies: No dependencies

FMT_SMF.1.1 - The TSF shall be capable of performing the following security management functions [*to administer the TOE locally and remotely and has the*

- *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UID.1 and FIA_UAU.2;*
- *Ability to configure the cryptographic functionality;*

(C) 2024 Adva Network Security GmbH. All rights reserved.

].

CC - FMT_SMR.2 Restrictions on security roles

This section describes the SFRs FMT_SMR.2 Restrictions on Security Roles:

Hierarchical to: FMT_SMR.1 Security roles.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.2.1 The TSF shall maintain the roles: [*Security Administrator*].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [

- *Security Administrator role shall be able to administer the TOE remotely;*

] are satisfied.

Application Note: The Security Administrator can administer the TOE through a remote mechanism (SSH, HTTPS/TLS, SNMPv3).

6.1.5 Class FPT – Protection of the TSF

CC - FPT_APW_EXT.1 Protection of administrator passwords

See section 5.1 Extended TOE Security functional component for details.

CC - FPT_STM.1 Reliable time stamps

This section describes the SFRs FPT_STM.1 Reliable Time Stamps:

Hierarchical to: No other components.
Dependencies: No dependencies.

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

Application Note: The TSF does not provide reliable information about the current time at the TOE's location by itself, but depends on external time and date information provided manually by the administrator. The term 'reliable time stamps' refers to the strict use of the time and date information, that is provided externally, and the logging of all changes to the time settings including information about the old and new time. With this information the real time for all audit data can be calculated.

CC - FPT_TST_EXT.1 TSF Testing – extended

See section 5.1 Extended TOE Security functional component for details.

(C) 2024 Adva Network Security GmbH. All rights reserved.

6.1.6 Class FTA – TOE Access

CC - FTA_SSL.3 TSF-initiated Termination

This section describes the SFRs FTA_SSL.3 TSF-initiated Termination:

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate **a local or remote** interactive session after a [*Security Administrator-configurable time interval of session inactivity*].

Note, since SNMPv3 administration is session-less, this requirement does not apply to that user type.

CC - FTA_SSL.4 User-initiated termination

This section describes the SFRs FTA_SSL.4 User-initiated Termination:

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.4.1 The TSF shall allow **Security Administrator**-initiated termination of the **Security Administrator** own interactive session.

CC - FTA_TAB.1 Default TOE access banners

This section describes the SFRs FTA_TAB.1 Default TOE Access Banners:

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_TAB.1.1 - Before establishing **a Security Administrator** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

Application Note: This requirement is intended to apply to interactive sessions between a human user and a TOE. IT entities establishing connections or programmatic connections (e.g., remote procedure calls over a network) are not required to be covered by this requirement.

(C) 2024 Adva Network Security GmbH. All rights reserved.

6.1.7 Class FTP – Trusted path/channels

CC - FTP_TRP.1 Trusted path

This section describes the SFRs FTP_TRP.1 Trusted Path:

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_TRP.1.1 - The TSF shall be capable of using [*SSH, TLS, HTTPS*] to provide a communication path between itself and **authorized** [remote] **Security Administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [disclosure, [*and provides detection of modification of the channel data*]].

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

FTP_TRP.1.3 - The TSF shall require the use of the trusted path for [initial **Security Administrator** auth entication, [*and all remote administration actions*]].

Application Note: This requirement ensures that authorized remote administrators initiate all communication with the TOE via a trusted path, and that all communication with the TOE by remote administrators is performed over this path. The data passed in this trusted communication channel are encrypted as defined by the protocol chosen in the first selection.

6.2 Security assurance requirements

There are no TOE security assurance components.

7 TOE summary specification (C)

This chapter presents an overview of the implemented TOE security functionality.

7.1 TOE security functions list (I)

Find here the list of the supported security functions:

- Protected Communications
- System Monitoring
- TOE Administration
- Identification and Authentication
- Password mechanism
- Session Timeouts
- TSF Self test

(C) 2024 Adva Network Security GmbH. All rights reserved.

7.2 TOE security functions rationale (I)

The specification of the TOE security functions refers directly to the TOE security requirements. The following table displays the correlation between security requirements and security functions.

Table 14: TOE security functions rationale

Security functional requirements vs. security functions	Protected communi-cations	System moni-toring	TOE admini-stration	Identifica-tion and authenti-cation	Password mecha-nism	Session timeouts	TSF Self test
FAU_GEN.1		X					
FAU_GEN.2		X					
FAU_GEN.1	X						
FCS_CKM.1	X						
FCS_CKM.2	X						
FCS_CKM.4	X						
FCS_COP.1(1)	X						
FCS_COP.1(2)	X						
FCS_COP.1(3)	X						
FCS_COP.1(4)	X						
FCS_TLSS_EXT.1	X						
FCS_SSHS_EXT.1	X						
FCS_HTTPS_EXT.1	X						
FIA_PMG_EXT.1			X		X		
FIA_UID.1			X	X			
FIA_UAU.2			X	X			
FIA_UAU.7			X	X			
FMT_MTD.1			X	X			

(C) 2024 Adva Network Security GmbH. All rights reserved.

FMT_SMF.1			X	X			
FMT_SMR.2			X	X			
FPT_APW_EXT.1			X		X		
FPT_STM.1		X					
FPT_TST_EXT.1							X
FTA_SSL.3			X			X	
FTA_SSL.4			X			X	
FTA_TAB.1			X				
FTP_TRP.1	X			X			

7.3 TOE security functions details (I)

7.3.1 Protected communications

Sensitive data to and from the TOE is transmitted encrypted. The TOE provides encryption for the communication paths between itself and the endpoint using standard protocols:

- HTTPS (with TLS encryption), and **(FCS_HTTPS_EXT.1, FCS_TLS_EXT.1)**
- SSH **(FCS_SSH_EXT.1)**
- SNMPv3 (**FCS_COP.1(1)**).

All protocols (SSH, HTTPS/TLS, SNMPv3) are specified by RFCs. The requirements have been imposed on some specifications for cryptographic primitives to provide interoperability and resistance to cryptographic attack. **(FCS_CKM.1)** This comprises cryptographic operations used for encryption and decryption **(FCS_COP.1(1))**, for cryptographic signatures **(FCS_COP.1(2))**, for hashing **(FCS_COP.1(3))** and for keyed-hash message authentication **(FCS_COP.1(4))**.
Cryptographic keys are destroyed when the keys are no longer required. **(FCS_CKM.4)**
When the administrator uses a remote connection to administrate the TOE, a trusted channel is established. Over this channel the initial administrator authentication and all remote administration actions are transmitted. **(FTP_TRP.1)**.

(C) 2024 Adva Network Security GmbH. All rights reserved.

7.3.2 System monitoring

The System monitoring function provides the TOE with the functionality of generating audit records to assure that information exists that allows administrators to discover intentional and unintentional issues with the configuration and/or operation of the system, the TOEs generates audit data targeted at detecting such activity.

All events logged by the audit functions are listed in Table 14. (**FAU_GEN.1**)

The log entries contain date and time of the event (**FPT_STM.1**), type of event, subject identity (if applicable), and the outcome (success or failure) of the event. When an authenticated user triggers an auditable event, the identity of that user is also logged. (**FAU_GEN.2**)

7.3.3 TOE administration

In order to provide a trusted means for administrators to interact with the TOE, the TOE provides a password-based logon mechanism. The TOE supports strong passwords and avoids attacks by observing a password being typed by an administrator. Session termination mitigates the risk of an account being used illegitimately. Passwords are stored unreadable and there must be no interface provided for specifically reading the password or password file such that the passwords are displayed in plain text.

7.3.4 Identification and authentication

To gain access to the TOE, either by SSH or by Web Session, administrators must log on with a user account and password. When a user connects to the TOE an advisory notice and consent warning message is displayed regarding use of the TOE. A plain text message is displayed when the user connects via SSH or a web page when the user connects via a Web Session. (**FTA_TAB.1**) After that the user can enter his credentials.

The login authentication process on the TOE will verify the entered credentials against account information that is stored locally on the TOE. (**FIA_UID.1**, **FIA_UAU.2**, **FIA_UAU.7**)

If the entered credentials match the stored account information (**FMT_MTD.1**), the user is granted access and assigned administrative privileges associated with their user account. (**FMT_SMR.2**) The authentication mechanism is maintained by the TOE itself.

An administrator (authorized user) can administer the TOE locally and remotely and is able to perform following administrative actions: (**FMT_SMF.1**, **FMT_SMR.2**)

(C) 2024 Adva Network Security GmbH. All rights reserved.

· Ability to configure a list of services available before an entity is identified and authenticated
· Ability to configure the cryptographic functionality

The system is delivered with a single user account. This user account has administrative privileges and can be used to create other accounts.

7.3.4.1 Password mechanism

The TOE stores passwords in non-plaintext form and prevents the reading of plaintext passwords. The passwords entered during logon are obscured for SSH (invisible text echo) as well as Web session logons (password field used in web form). **(FPT_APW_EXT.1)**
The TOE password management capabilities for administrative passwords allow passwords to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “(”, “)”, [“_” , “+” , “|” , “~” , “{”, “ }” , “[” , “]” , “-”, “.”]. The minimum password length can be specified by the administrator and support passwords of 15 characters or greater. **(FIA_PMG_EXT.1)**

7.3.4.2 Session timeouts

Any uncompleted login attempt or active session will be terminated after a defined period of inactivity. **(FTA_SSL.3, FTA_SSL.4)**. The following table provides an overview of which types of access can be configured and range values available for configuring timeouts.

Table 15: Session and login timeouts

Type of access	Range in seconds	Default
SSH Login	5 - 300 s	30 s
Web Session	30 - 3600 s	900 s

7.3.5 TSF Self test

The TOE performs several self tests of following TSF during initial start-up **(FPT_TST_EXT.1)**:

- The consistency of the File system.
- The consistency of the Database.
- The software integrity check (only NCU-3 support). It validates software integrity on the file system, by verifying the current state of the constant files on the root partition against the manifest file that was generated and included in the software as part of the build process. The manifest contains the following information:
  - executable binary files
  - executable text files (scripts);
  - shared libraries

(C) 2024 Adva Network Security GmbH. All rights reserved.

    - all constant files on root partition
    - SHA-384 hashes for comparison
    - Ownership for comparison
    - file permissions for comparison
    - failure results in non-operational state
- The file system integrity check (only NCU-II support):
    - mounts (creates) basic virtual RAM file systems
    - verifies and mounts the non-volatile file system
    - verifies and mounts the active or standby software partition file system
    - failures here may result in non-operational state. System is designed to automatically attempt to fix and continue if errors are found.

Self tests or any other action on the module cause alarms to be raised. They become important especially when the self tests result in failure conditions, which require user intervention to recover normal operation. The alarms are logged and can be tracked from there. If everything starts up properly and db checking passes the verification there is no explicit evidence that all the checking and db verifications were performed.

(C) 2024 Adva Network Security GmbH. All rights reserved.

8 Appendix

8.1 Icons

Table 16: Icon definition

Icon	Definition
	Assumption (A)
	Objective (O/OE)
	Organizational security policy (OSP)
	Rationale (Rat)
	Security functional requirement
	Threat (T)
	TOE Security Function

8.2 References

CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 • Part 1: Introduction and general model, CCMB-2017-04-001, • Part 2: Security functional requirements, CCMB-2017-04-002, • Part 3: Security Assurance Requirements,CCMB-2017-04-003.
CPP-ND	Collaborative Protection Profile for Network Devices, Version 1.0, 27. February 2015

8.3 Glossary

A	assumption	
C	Common	marks sections with content applicable to several products/TOEs
CC	Common Criteria	
CCC	Common criteria certification	

(C) 2024 Adva Network Security GmbH. All rights reserved.

CI	Corporate Identity	
EMI	Electro-magnetic interference	
EAL	Evaluation Assurance Level	
FPGA	Field programmable gate array	type of logic IC
FSP	Fiber Service Platform	product family name
FW	Firmware	
GUI	Graphical user interface	
HW	Hardware	
I	Individual	marks sections with content applicable to one specific product/TOE
ISO/OSI	International standards organisation/open systems interconnection	Open Systems Interconnection model: layer model for network protocol architectures
IT	Information technology	
ITU-T		Telecommunication standardization sector of Interational Telecommunication Union
KDF	Key Derivation Function	
KEM	Key Encapsulation Method	
LED	Light emitting diode	
MAC	Message Authentication Code	
n/a	not applicable	
NCU	Network Control Unit	controller module serving one node of FSP 3000R7
O	Objective	
OE	Operational environment	
OS	Operating system	
OSP	Organizational security policy	
PQC	Post-quantum cryptography	
PP	Protection profile	

(C) 2024 Adva Network Security GmbH. All rights reserved.

PRNG	Pseudo random number generator	
RNG	Random number generator	
RSASSA-PSS	Probabilistic signature scheme	
Rxx.x/Rxx.x.x	Release xx.x.x	release numbering of FSP 3000R7 (each x is a placeholder of one digit, example: R20.3.1)
SAR	Security assurance requirement	
SCU	Shelf Control Unit	controller module serving one chassis of FSP 3000R7
SE	Societas europaea	
SF	Security function	
SFP	Security function policy	
SFR	Security functional requirement	
ST	Security Target	
T	Threat	
TOE	Target of evaluation	
TRNG	True random number generator	physical/true random number generator
TSF	TOE security function	
TSFI	TSF interface	
WDM	Wavelength Division Multiplexing	method of extending data transport capability of optical systems

(C) 2024 Adva Network Security GmbH. All rights reserved.