Alcatel-Lucent Enterprise OmniSwitches with AOS 6.7.1.R04 and AOS 8.3.1.R01 Security Target

Version:	**1.0**
Part Number:	**014566-00**
Status:	**Final**
Last Update:	**2017-09-29**
Classification:	**Public**

Trademarks

atsec® is a trademark of atsec information security corporation in the United States, other countries, or both.

Omniswitch® is a trademark used by ALE USA Inc.

VxWorks® is a trademark of Wind River Systems.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
1.0	2017-09-29	Alejandro Masino	First version

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	Alcatel-Lucent Enterprise OmniSwitches with AOS 6.7.1.R04 and AOS 8.3.1.R01 Security Target
Version:	1.0
Part Number:	014566-00
Status:	Final
Date:	2017-09-29
Sponsor:	ALE USA Inc.
Developer:	ALE USA Inc.
Certification Body:	CSEC
Certification ID:	CSEC 2016007
Keywords:	ALE USA Inc., ALE, Alcatel-Lucent Enterprise, OmniSwitch, Alcatel-Lucent Operating System, AOS, OmniSwitch 6250, OmniSwitch 6350, OmniSwitch 6450, OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900, OmniSwitch 9900, OmniSwitch 10K, OS6250, OS6350, OS6450, OS6860, OS6865, OS6900, OS9900, OS10K

1.2 TOE Identification

The TOE is Alcatel-Lucent Enterprise OmniSwitches with AOS 6.7.1.79.R04 and AOS 8.3.1.348.R01.

1.3 TOE Type

The TOE type is network switch.

1.4 TOE Overview

The Target of Evaluation (TOE) is a network switch comprised of hardware and firmware/software.

The firmware/software is named Alcatel-Lucent Operating System (AOS) which is the single purpose operating system that operates the management functions of all of the Alcatel-Lucent Enterprise OmniSwitch switches. The evaluation covers AOS 6.7.1.79.R04, which is based on the VxWorks version 5.5.1 operating system, and AOS 8.3.1.348.R01, which is based on the Linux version 3.10.34 operating system.

The TOE hardware consists of the following families/series.

Family / Series	AOS Version	Processors
OmniSwitch 6250 (OS6250)	AOS 6.7.1.79.R04	Integrated ARMv5 core
OmniSwitch 6350 (OS6350)	AOS 6.7.1.79.R04	Integrated ARMv7 core
OmniSwitch 6450 (OS6450)	AOS 6.7.1.79.R04	Integrated ARMv5 core
OmniSwitch 6860 (OS6860)	AOS 8.3.1.348.R01	Cortex ARM 9

Family / Series	AOS Version	Processors
OmniSwitch 6865 (OS6865)	AOS 8.3.1.348.R01	Cortex ARM 9
OmniSwitch 6900 (OS6900)	AOS 8.3.1.348.R01	Freescale PowerPC MPC8572 or PowerPC P2040 (depending on model)
OmniSwitch 9900 (OS9900)	AOS 8.3.1.348.R01	Intel Atom C2518 (for CMM modules) and Intel Atom C2338 (for NI modules)
OmniSwitch 10K (OS10K)	AOS 8.3.1.348.R01	Freescale PowerPC MPC8572 (for both CMM and NI modules)

Table 1: TOE Hardware Configurations

The TOE provides Layer-2 switching, Layer-3 routing, and traffic filtering. Layer-2 switching analyzes incoming frames and makes forwarding decisions based on information contained in the frames. Layer-3 routing determines the next network point to which a packet should be forwarded toward its destination. These devices may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Routing protocols include Border Gateway Protocol (BGP), Routing Information Protocol (RIP) v.2, and Open Shortest Path First (OSPF). Filtering controls network traffic by controlling whether packets are forwarded or blocked at the switch’s interfaces. Each packet is examined to determine whether to forward or drop the packet, on the basis of the criteria specified within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

The Alcatel-Lucent Enterprise OmniSwitch 6250 Series are stackable Layer-2+ Fast Ethernet Local Area Network (LAN) value switches for both the enterprise and Ethernet access segment. They allow for any mix of Power over Ethernet (PoE) and non-PoE, up to 416 ports. They provide advanced Layer-2+ features with basic Layer-3 routing for both IPv4 and IPv6.

The Alcatel-Lucent Enterprise OmniSwitch 6350 Series are stackable, fixed-configuration managed Gigabit Ethernet (GigE) switches available in 10, 24 and 48-port, non-PoE and PoE models. They provide advanced Layer-2+ features with basic Layer-3 routing for both IPv4 and IPv6.

The Alcatel-Lucent Enterprise OmniSwitch 6450 Series are stackable Fast Ethernet and GigE LAN value switches offering versatile 10, 24 and 48-port fixed configuration switches with 10 GigE uplinks and provide upgrade paths for 10 GigE stacking, 10 GigE uplinks and metro Ethernet services. They provide advanced Layer-2+ features with basic Layer-3 routing for both IPv4 and IPv6.

The Alcatel-Lucent Enterprise OmniSwitch 6860 Series are stackable LAN switches that are compact, high-density GigE and 10 GigE platforms designed for the most demanding converged networks. They provide Quality of Service (QoS), access control lists (ACLs), Layer-2 / Layer-3 switching, virtual LAN (VLAN) stacking and IPv6.

The Alcatel-Lucent Enterprise OmniSwitch 6865 Series are stackable LAN switches that are compact, industrial-grade, high-density GigE and 10 GigE platforms designed to operate reliably in severe temperatures, as well as harsh physical and electrical conditions. They provide QoS, ACLs, Layer-2 / Layer-3 switching, VLAN stacking and IPv6.

The Alcatel-Lucent Enterprise OmniSwitch 6900 Series are stackable LAN and data center switches that are compact, high-density 10 GigE and 40 GigE platforms. They provide Virtual Extensible Local Area Network (VXLAN), OpenFlow, Shortest Path Bridging (SPB), Data Center Bridging (DCB) capabilities, QoS, Layer-2 and Layer-3 switching, as well as system and network level resiliency.

The Alcatel-Lucent Enterprise OmniSwitch 9900 Series are modular LAN chassis platform, high-capability, and high-performance modular Ethernet LAN switches for enterprise, service provider and data center environments. They provide uninterrupted network uptime with non-stop Layer-2 and Layer-3 forwarding. They also provide the capability to optimize/simplify Layer-2 and Layer-3 network designs, and reduce administration overhead while increasing network capacity with resilient multipath active-active dual homing multi-chassis support.

The Alcatel-Lucent Enterprise OmniSwitch 10K Series are modular LAN chassis platform, high-density switches. They include non-blocking 10/40 GigE ports with large packet buffers and high-density (10/100/1000) ports. They provide uninterrupted network uptime with non-stop Layer-2 and Layer-3 forwarding and in-service software upgrades. They also provide the capability to optimize/simply the Layer-2 and Layer-3 network deployments.

1.4.1 Intended method of use

The intended TOE environment is a secure data center that protects the TOE from unauthorized physical access. Only security administrators are to have access to connect to the serial console, or gain physical access to the hardware storing log data. Appropriate administrator security policy and security procedure guidance must be in place to govern operational management of the TOE within its operational environment.

The TOE is not intended for use as a general purpose computer and only executes the services needed to perform its intended function.

1.4.2 Major security features

The TOE provides the following security functions.

- Generation of audit records for security related events, which can be locally stored or sent to a remote server
- Cryptographic support for protecting TOE Security Functionality (TSF) data and for establishing secure protocols used by the TOE
- Identification and authentication of Security Administrators that access the TOE for Security Management purposes
- Security management, supporting TSF data configuration through local and remote sessions
- Protection of the TSF, through the establishment of secure channels between the TOE and external IT entities, remote consoles or other devices in the network

1.5 TOE Description

1.5.1 Architecture

The following diagram shows the basic components that comprise the TOE.

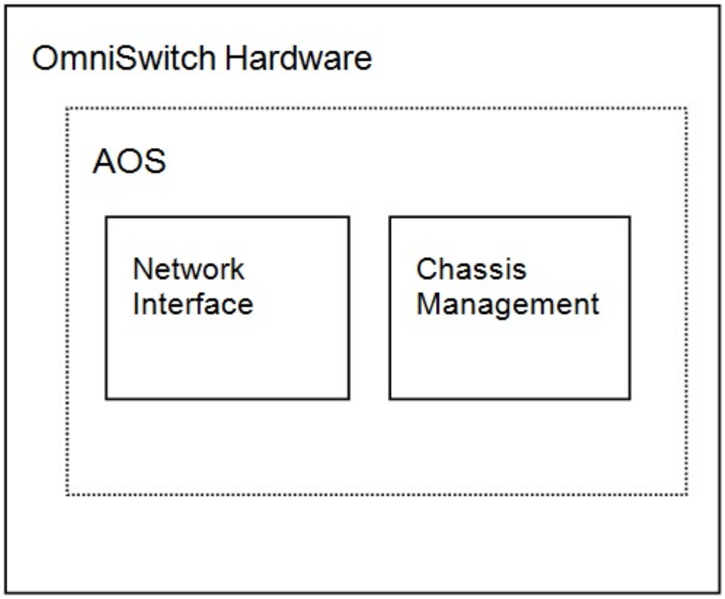

Figure 1: TOE Architecture

The term Chassis Management Module (CMM) is used to describe the logical management functionality of the TOE providing the following services.

- Console, Universal Serial Bus (USB), and Ethernet management port connections to the switch. The console port that is used to connect a serial console to initialize and configure the TOE via a Command Line Interface (CLI). Depending on the TOE model the physical interface can be an USB or an RJ-45 connector.
- Software and configuration management, including the CLI
- Power distribution
- Switch diagnostics
- Important availability features, including failover (when used in conjunction with another CMM), software rollback, temperature management, and power management

Network Interface (NI) modules provides the connectivity to the network through different physical ports, connector types and speed. The NI modules are categorized into Gigabit Ethernet Network Interface (GNI), 10-Gigabit Ethernet Network Interface (XNI) and 40-Gigabit Ethernet Network Interface (QNI) modules. GNI modules provide 1000 Mbps (1 Gbps) connections. GNI modules can be used for backbone connections in networks where Gigabit Ethernet is used as the backbone media. XNI modules provide up to six 10000 Mbps (10 Gbps) connections per module and can be used in networks where 10-gigabit Ethernet is used as the backbone media. Finally, QNI modules provide 40000 Mbps (40 Gbps) connections per module.

The main distinction between the hardware models are the form factor (either chassis or stacks), the number of physical ports, the port speeds, the connector types, and the amount of physical RAM installed.

The OS6250, OS6350, and OS6450 Series products are packaged in a 1U housing with a single Printer Circuit Board (PCB) with an integrated Advanced RISC Machines (ARM) version 5 / ARM version 7 CPU. The CMM and NI functions execute on this processor, and communicate via a socket based protocol running over TCP/IP. The 1U units (6250, 6450) are stackable, having special purpose connectors that allow up to eight units to be connected together and act as a single unit where each unit supporting the CMM and NI functions on a single processor. For OS6350, the number of units that can be stacked is four.

The OS6860, OS6865, OS6900, OS9900, and OS10K Series products are stackable units. The OS6865, OS9900 and OS10K stackable products may have up to two units, the OS6900 stackable products may have up to six units, and the OS6860 stackable products may have up to eight units. The OS10K/OS9900 units support CMM and NI functions on different processor while the OS6900/OS6860 units supporting the CMM and NI functions on a single processor.

The OS6860 series products are packaged in a single PCB with an embedded CPU Cortex ARM 9 processor. The CMM and NI functions execute on this processor, and communicate via a socket based protocol running over TCP/IP. A maximum of eight 6860 units can be stacked to form a Virtual-Chassis through the 10G or 21G links connected between the units. They act as a single unit after forming Virtual-chassis.

The OS6900 series products are packaged in a single PCB with a Freescale MPC8572/P2040 PowerPC processor. The CMM and NI functions execute on this processor, and communicate via a socket based protocol running over TCP/IP. The OS6900 units are stackable units that form a Virtual-Chassis connected through 10G or 40G links. A maximum of six 6900 units can be stacked to the Virtual-Chassis, which acts as a single unit.

The OS9900 is a chassis based product including a CMM with an Intel Atom (Rangeley) C2518 processor. The CMM functions execute on this processor and communicate with the NIs via a socket based protocol running over TCP/IP. This product can support up to six NI cards with an Intel Atom (Rangeley) C2338 processor, where the NI functions execute. The OS9900 units are stackable units that form a Virtual-Chassis connected through 10G or 40G links provided by the NI cards. Two OS9900 units can be stacked to the Virtual-Chassis, which acts as a single unit.

The OS10K is a chassis based product including a CMM with a Freescale MPC8572 PowerPC processor. The CMM functions execute on this processor and communicate with the NIs via a socket based protocol running over TCP/IP. OS10K can support up to eight NI cards with a Freescale MPC 8572 PowerPC processor where the NI functions execute. The OS10K units are stackable units that form a Virtual-Chassis through 10G or 40G links provided by the NI cards. Two OS10K units can be stacked to the Virtual-Chassis, which acts as a single unit.

1.5.2 TOE boundaries

1.5.2.1 Physical

Figure 2 shows a depiction of the TOE and its operating environment. The red dotted lines enclose the TOE physical boundary.

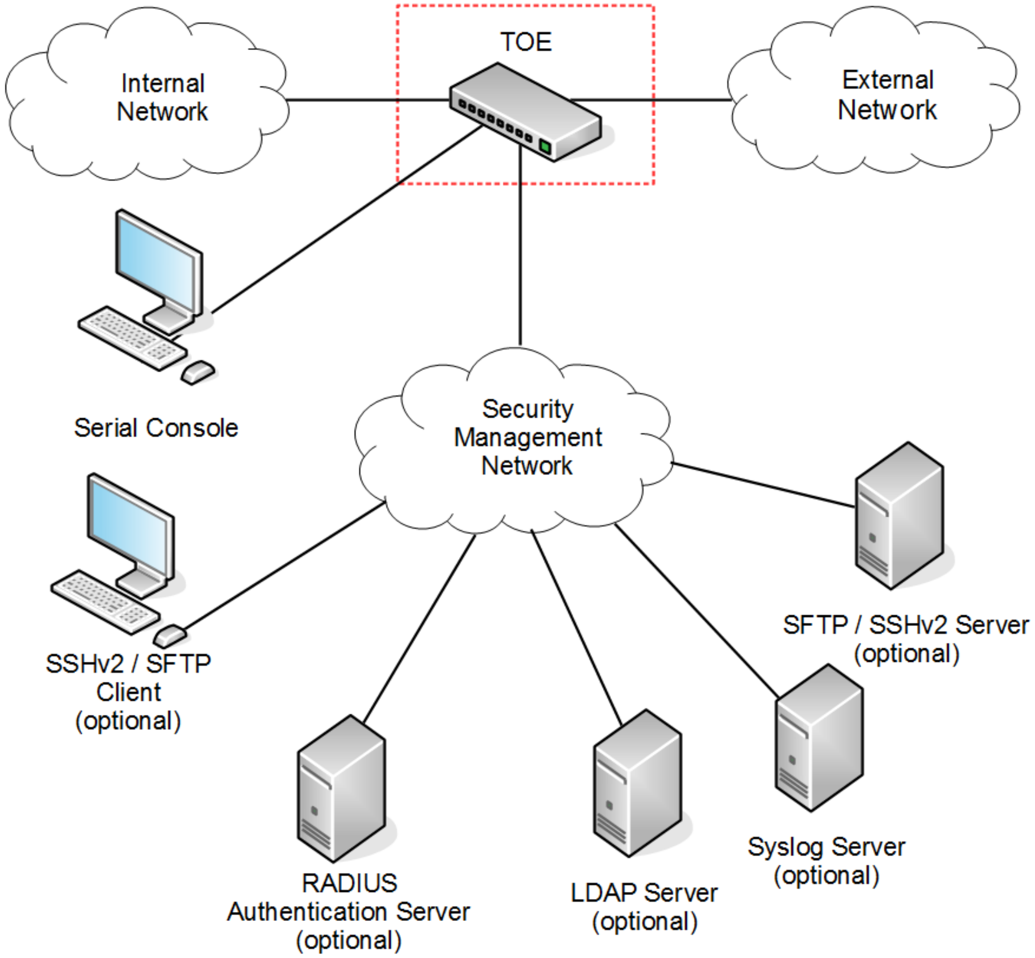
TOE
Internal Network
External Network
Serial Console
Security Management Network
SFTP / SSHv2 Server (optional)
SSHv2 / SFTP Client (optional)
Syslog Server (optional)
RADIUS Authentication Server (optional)
LDAP Server (optional)

Figure 2: TOE Boundary

1.5.2.1.1 Hardware / Software Components

Table 2 below specifies the TOE hardware and software components that can be combined to form valid TOE configurations. Please notice that the acronym SFP is referring to Small Form Factor Pluggable transceivers; this should not be confused with the same CC acronym that refers to Security Function Policies.

Family Series	Software ID	Hardware ID	Description
OmniSwitch 6250	AOS 6.7.1.79.R04	OS6250-8M	Fast Ethernet chassis in a 1U half-rack form factor with eight RJ-45 ports configurable to 10/100Base-T, two SFP/RJ-45 combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X and two SFP+ fiber ports with 1G uplink or 2.5G stacking capability. It has an internal AC power supply.

Family Series	Software ID	Hardware ID	Description
		OS6250-24M	Fast Gigabit Ethernet chassis in a 1U half-rack form factor with twenty-four RJ-45 ports configurable to 10/100Base-T, two RJ-45/SFP combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X and two SFP+ fiber ports with 1G uplink or 2.5G stacking capability. It has an internal AC power supply, and optional redundant external power supply.
		OS6250-24MD	Fast Gigabit Ethernet chassis in a 1U half-rack form factor with twenty-four RJ-45 ports configurable to 10/100Base-T, two RJ-45/SFP combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X and two SFP+ fiber ports with 1G uplink or 2.5G stacking capability. It has an internal DC power supply, and optional redundant external power supply.
		OS6250-24	Fast Ethernet chassis in a 1U form factor with twenty-four RJ-45 ports configurable to 10/100Base-T, two RJ-45/SFP combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X and two dedicated 2.5G HDMI stacking ports. It has an internal AC power supply, and optional redundant external power supply.
		OS6250-P24	Fast Ethernet chassis in a 1U half-rack form factor twenty-four PoE RJ-45 ports configurable to 10/100Base-T, two SFP/PoE RJ-45 combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X and two dedicated 2.5G HDMI stacking ports. It has external primary and redundant power supplies.
OmniSwitch 6350	AOS 6.7.1.79.R04	OS6350-10	Provides eight 10/100/1000BaseT Ethernet ports, two RJ-45/SFP combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X for uplink capability. It has an internal AC power supply.
		OS6350-P10	Provides eight 10/100/1000BaseT PoE Ethernet ports, two RJ-45/SFP combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X for uplink capability. It has an internal AC power supply.
		OS6350-24	Gigabit Ethernet standalone chassis in a 1U form factor with twenty-four 10/100/1000 Base-T ports, four gigabit SFP ports. Two of the SFP ports can optionally provide 5G stacking capability. It has an internal AC power supply.
		OS6350-P24	Gigabit Ethernet standalone chassis in a 1U form factor with twenty-four 10/100/1000 PoE Base-T ports, four gigabit SFP ports. Two of the SFP ports can optionally provide 5G stacking capability. It has an internal AC power supply.
		OS6350-48	Gigabit Ethernet standalone chassis in a 1U form factor with forty-eight 10/100/1000 Base-T ports, four gigabit SFP ports. Two of the SFP ports can optionally provide 5G stacking capability. It has an internal AC power supply.

Family Series	Software ID	Hardware ID	Description
		OS6350-P48	Gigabit Ethernet standalone chassis in a 1U form factor with forty-eight 10/100/1000 PoE Base-T ports, four gigabit SFP ports. Two of the SFP ports can optionally provide 5G stacking capability. It has an internal AC power supply.
OmniSwitch 6450	AOS 6.7.1.79.R04	OS6450-10	Provides eight 10/100/1000BaseT Ethernet ports, two RJ-45/SFP combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X, and two SFP ports with uplink capability. It has an internal AC power supply.
		OS6450-10L	Provides eight 10/100BaseT Ethernet ports upgradeable to 10/100/1000BaseT, two RJ-45/SFP combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X, and two SFP ports with uplink capability. It has an internal AC power supply.
		OS6450-10M	Provides eight 10/100/1000BaseT Ethernet ports, two RJ-45/SFP combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X, two SFP ports with uplink capability, and factory-enabled Metro support. It has an internal AC power supply.
		OS6450-P10	Provides eight 10/100/1000BaseT PoE ports, two RJ-45/SFP combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X, and two SFP ports with uplink capability. It has an internal AC power supply.
		OS6450-P10L	Provides eight 10/100BaseT PoE ports upgradeable to 10/100/1000BaseT, two RJ-45/SFP combo ports configurable to be 10/100/1000Base-T or 100/1000Base-X, and two SFP ports with uplink capability. It has an internal AC power supply.
		OS6450-P10S	Provides four 10/100BaseT Power over HD Base-T (PoH) ports (up to ~75W per port), four 10/100BaseT PoE ports, and two 100FX/1000-X fixed fiber ports. This switch also supports IEEE 1588 Precision Time Protocol (PTP). It has an internal AC power supply.
		OS6450-24	Provides twenty-four 10/100/1000 BaseT ports, two fixed SFP+ ports with uplink capability, and one expansion slot for optional stacking or uplink modules. It includes an internal AC power supply and an internal slot for optional AC or DC backup power.
		OS6450-24L	Provides twenty-four 10/100 BaseT ports upgradeable to 10/100/1000BaseT, two fixed SFP+ ports with uplink capability, and one expansion slot for optional stacking or uplink modules. It includes an internal AC power supply and an internal slot for optional AC or DC backup power.

Family Series	Software ID	Hardware ID	Description
		OS6450-24X	Provides twenty-four 10/100/1000 BaseT ports, two fixed SFP+ ports and one expansion slot for optional stacking or uplink modules. 10G uplink speed feature enabled by default. It includes an internal AC power and an internal slot for optional internal AC or DC backup power.
		OS6450-24XM	Provides twenty-four 10/100/1000 BaseT ports, two fixed SFP+ ports and one expansion slot for optional stacking or uplink modules. 10G uplink speed and Metro features enabled by default. It includes an internal AC power and an internal slot for optional internal AC or DC backup power.
		OS6450-P24	Provides twenty-four PoE 10/100/1000 BaseT ports, two fixed SFP+ ports with uplink capability, and one expansion slot for optional stacking or uplink modules. It includes an internal AC power supply and a connector for external backup or PoE power supply.
		OS6450-P24L	Provides twenty-four PoE 10/100 BaseT ports upgradeable to 10/100/1000BaseT, two fixed SFP+ ports with uplink capability and one expansion slot for optional stacking or uplink modules. It includes an internal AC power supply and an internal slot for optional AC or DC backup power.
		OS6450-P24X	Provides twenty-four PoE 10/100/1000 BaseT ports, two fixed SFP+ports and one expansion slot for optional stacking or uplink modules. 10G uplink speed enabled by default. It includes an internal AC power with optional external AC backup power (installed on a separate 1 RU tray).
		OS6450-U24	Provides twenty-two 100/1000 Base-X SFP ports, two RJ-45/SFP combo ports configurable to be 10/100/1000 BaseT or 100/1000 Base-X, two fixed SFP+ ports with uplink capability and one expansion slot for optional stacking or uplink modules. It includes an internal AC power supply and an internal slot for optional AC or DC backup power.
		OS6450-U24S	Provides twenty-two 100/1000 Base-X SFP ports, two RJ-45/SFP 1G combo ports, two 10G fixed fiber SFP+ ports, and one expansion slot for optional stacking or uplink modules. It includes an internal AC power supply and an internal slot for optional AC or DC backup power. This switch also supports IEEE 1588 PTP.
		OS6450-U24SXM	Provides twenty-two 100/1000 Base-X SFP ports, two RJ-45/SFP 1G combo ports, two 10G fixed fiber SFP+ ports, one expansion slot for optional stacking or uplink modules, and factory-enabled 10G uplink and Metro support. It includes an internal AC power supply and an internal slot for optional AC or DC backup power. This switch also supports IEEE 1588 PTP.

Family Series	Software ID	Hardware ID	Description
		OS6450-U24X	Provides twenty-two 100/1000 Base-X SFP ports, two RJ-45 / SFP combo ports configurable to be 10/100/1000 BaseT or 100/1000 Base-X, and one expansion slot for optional stacking or uplink modules. 10G uplink speed enabled by default. It includes an internal AC power supply and an internal slot for optional AC or DC backup power.
		OS6450-48	Provides forty-eight 10/100/1000 BaseT ports, two fixed SFP+ ports with uplink capability and one expansion slot for optional stacking or uplink modules. It includes an internal AC power supply and an internal slot for optional AC or DC backup power.
		OS6450-48L	Provides forty-eight 10/100 BaseT ports upgradeable to 10/100/1000BaseT, two fixed SFP+ ports with uplink capability and one expansion slot for optional stacking or uplink modules. It includes an internal AC power supply and an internal slot for optional AC or DC backup power.
		OS6450-48X	Provides forty-eight 10/100/1000 BaseT ports, two fixed SFP+ ports with uplink capability, one expansion slot for optional stacking or uplink modules, and factory-enabled 10G uplink support. It includes an internal AC power supply and an internal slot for optional AC or DC backup power.
		OS6450-P48	Provides forty-eight PoE 10/100/1000 BaseT ports, two fixed SFP+ ports with uplink capability and one expansion slot for optional stacking or uplink modules. It includes an internal AC power supply and a connector for external backup or PoE power supply.
		OS6450-P48L	Provides forty-eight PoE 10/100 BaseT ports upgradeable to 10/100/1000BaseT, two fixed SFP+ ports and one expansion slot for optional stacking or uplink modules. It includes an internal AC power supply and a connector for external backup or PoE power supply.
		OS6450-P48X	Provides forty-eight PoE 10/100/1000BaseT ports, two fixed SFP+ ports and one expansion slot for optional stacking or uplink modules. 10G uplink speed enabled by default. It includes an internal AC power supply and optional external AC backup power (installed on a separate 1 RU tray).
OmniSwitch 6860	AOS 8.3.1.348.R01	OS6860-24	Fixed-configuration chassis in a 1U form factor with twenty-four 10/100/1000 Base-T ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports.
		OS6860-P24	Fixed-configuration chassis in a 1U form factor with twenty-four 10/100/1000 Base-T PoE ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports.
		OS6860-48	Fixed-configuration chassis in a 1U form factor with forty-eight 10/100/1000 Base-T ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports.

Family Series	Software ID	Hardware ID	Description
		OS6860-P48	Fixed-configuration chassis in a 1U form factor with forty-eight 10/100/1000 Base-T PoE ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports.
		OS6860E-24	Fixed-configuration chassis in a 1U form factor with twenty-four 10/100/1000 Base-T ports, four fixed SFP+ (1G/10G) ports and two 20G virtual Chassis link ports. Includes a built-in co-processor for Enhanced network services.
		OS6860E-P24	Fixed-configuration chassis in a 1U form factor with twenty-four 10/100/1000 Base-T PoE ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports. Includes a built-in co-processor for Enhanced network services.
		OS6860E-48	Fixed-configuration chassis in a 1U form factor with forty-eight 10/100/1000 Base-T ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports. Includes a built-in co-processor for Enhanced network services.
		OS6860E-P48	Fixed-configuration chassis in a 1U form factor with forty-eight 10/100/1000 Base-T PoE ports, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports. Includes a built-in co-processor for Enhanced network services.
		OS6860E-U28	Fixed-configuration chassis in a 1U form factor with 28 ports supporting 1000Base-X and 100Base-FX, four fixed SFP+ (1G/10G) ports and two 20G Virtual Chassis link ports. Includes a built-in co-processor for Enhanced network services.
OmniSwitch 6865	AOS 8.3.1.348.R01	OS6865-P16X	Hardened Stackable Gigabit Ethernet L3 fixed configuration switches for harsh temperature, physical and electrical conditions. It has twelve RJ-45 10/100/1000 Base-T ports with eight ports PoE+ and four ports 60W PoE capable, two 1000 Base-X SFP ports and two fixed SFP+ (1G/10G) ports. It provides SPBM, advanced routing and QOS capabilities. It also provides IEEE 1588v2 PTP capability on all ports.
OmniSwitch 6900	AOS 8.3.1.348.R01	OS6900-X20	10 Gb Ethernet L2/L3 fixed configuration chassis in a 1U form factor with twenty SFP+ ports, one optional module slot.
		OS6900-X40	10 Gb Ethernet L2/L3 fixed configuration chassis in a 1U form factor with forty SFP+ ports, two optional module slots.
		OS6900-X72	10 Gigabit / 40 Gigabit Ethernet L3 fixed configuration chassis in a 1U form factor with forty-eight 1/10G SFP+ ports and six 40G QSFP+ ports. QSFP+ ports operate as single 40GE port or Quad-10GE. Console and Ethernet management ports are RJ45.

Family Series	Software ID	Hardware ID	Description
		OS6900-T20	10 Gb Ethernet L2/L3 fixed configuration chassis in a 1U form factor with twenty 10GBase-T ports, auto-negotiable 100-BaseT, 1/10 GigE one optional module slot.
		OS6900-T40	10 Gb Ethernet L2/L3 fixed configuration chassis in a 1U form factor with forty 10GBase-T ports, auto-negotiable 100-BaseT, 1/10 GigE two optional module slots.
		OS6900-Q32	40 Gb Ethernet L3 fixed configuration chassis in a 1U form factor with thirty-two QSFP+ ports. Ports operate as single 40GigE port or Quad-10GigE.
OmniSwitch 9900	AOS 8.3.1.348.R01	OmniSwitch 9907 Chassis	The OmniSwitch 9900 chassis offers six slots for high-capacity 1/10/40-Gigabit Ethernet Network Interface (NI) modules. Additional slots are used for primary and redundant Chassis Management Modules (CMMs), Chassis Fabric Modules (CFMs), fan trays and power supplies. At least one CMM, an additional CMM or CFM , and one NI are required to assembly an operational network switch.
		OS99-CMM	This CMM includes a processor module, a fabric module, two 40G QSFP ports, and AOS software with advanced IP routing SW (IPv4/IPv6).
		OS9907-CFM	This CFM provides expanded switching fabric for the chassis, which increases switching throughput and provides redundancy.
		OS99-XNI-48	This 10 Gigabit network interface (XNI) card offers forty-eight wirerate 10GBase-T ports.
		OS99-XNI-U48	This XNI card offers forty-eight wirerate unpopulated SFP+ ports with 1/10 Gbps connections.
		OS99-GNI-48	This Gigabit network interface (GNI) card offers forty-eight wirerate RJ-45 10/100/1000Base-T ports.
		OS99-GNI-P48	This GNI card offers forty-eight wirerate RJ-45 10/100/1000Base-T ports with PoE.
OmniSwitch 10K	AOS 8.3.1.348.R01	OmniSwitch 10K Chassis	The OmniSwitch 10K chassis offers eight slots for high-capacity 1/10/40-Gigabit Ethernet Network Interface (NI) modules. Additional slots are used for primary and redundant CMMs, CFMs, fan trays and power supplies. At least one CMM, an additional CMM or CFM , and one NI are required to assembly an operational network switch.
		OS10K-CMM	This CMM includes a processor module, a fabric module, and AOS software with advanced IP routing SW (IPv4/IPv6).
		OS10K-CFM	This CFM provides expanded switching fabric for the chassis, which increases switching throughput and provides redundancy.

Family Series	Software ID	Hardware ID	Description
		OS10K-GNI-C48E	This Gigabit Ethernet Network Interface (GNI) module provides 1 Gbps connections, with forty-eight auto-sensing, auto-negotiating ports, individually configurable as 10BaseT, 100BaseTX, or 1000BaseT.
		OS10K-GNI-U48E	This GNI module provides 1 Gbps connections, with forty-eight SFP transceiver connectors.
		OS10K-XNI-U32S	This 10 Gigabit Network Interface (XNI) module provides varying 10 Gbps connections, with thirty-two SFP+ transceiver connectors.
		OS10K-XNI-U32E	This XNI module provides varying 10 Gbps connections, with thirty-two SFP+ transceiver connectors.
		OS10K-XNI-U16E	This XNI module provides varying 10 Gbps connections, with sixteen SFP+ transceiver connectors.
		OS10K-XNI-U16L	This XNI module provides varying 10 Gbps connections, with sixteen SFP+ transceiver connectors (this is a “Lite” module restricting 8 ports to 1G speed but can be upgraded to sixteen 10G ports).
		OS10K-QNI-U4E	This 40 Gigabit Network Interface (QNI) module provides varying 40 Gbps connections, with four QSFP+ transceiver connectors.
		OS10K-QNI-U8E	This QNI module provides varying 40 Gbps connections, with eight QSFP+ transceiver connectors.

Table 2: TOE Hardware / Software Components

1.5.2.1.2 TOE Guidance

The following documentation comprises the TOE guidance and is available on the Alcatel-Lucent Enterprise Service and Support website.

- OmniSwitch models with AOS 6.7.1.79.R04
  - Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 6.7.1.R04 [AOS6-CCGUIDE]
  - AOS Release 6.7.1 Release Notes [AOS6-RN]
  - OmniSwitch AOS Release 6250/6350/6450 Switch Management Guide [AOS6-SM]
  - OmniSwitch AOS Release 6250/6350/6450 CLI Reference Guide [AOS6-CLI]
  - OmniSwitch AOS Release 6250/6350/6450 Network Configuration Guide [AOS6-NC]
  - OmniSwitch 6250/6350/6450 Transceivers Guide [AOS6-TCV]
  - OmniSwitch 6250 Hardware Users Guide [OS6250-HWUG]
  - OmniSwitch 6350 Hardware Users Guide [OS6350-HWUG]
  - OmniSwitch 6450 Hardware Users Guide [OS6450-HWUG]
- OmniSwitch models with AOS 8.3.1.348.R01

- Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS 8.3.1.R01 [AOS8-CCGUIDE]
- AOS Release 8.3.1 Release Notes [AOS8-RN]
- OmniSwitch AOS Release 8 Switch Management Guide [AOS8-SM]
- OmniSwitch AOS Release 8 CLI Reference Guide [AOS8-CLI]
- OmniSwitch AOS Release 8 Network Configuration Guide [AOS8-NC]
- OmniSwitch AOS Release 8 Advanced Routing Configuration Guide [AOS8-ARC]
- OmniSwitch AOS Release 8 Transceivers Guide [AOS8-TCV]
- OmniSwitch AOS Release 8 Data Center Switching Guide [AOS8-DCS]
- OmniSwitch 6860 Hardware Users Guide [OS6860-HWUG]
- OmniSwitch 6865 Hardware Users Guide [OS6865-HWUG]
- OmniSwitch 6900 Hardware Users Guide [OS6900-HWUG]
- OmniSwitch 9900 Hardware Users Guide [OS9900-HWUG]
- OmniSwitch 10K Hardware Users Guide [OS10K-HWUG]
- OmniSwitch 10K Getting Started Guide [OS10K-GS]

1.5.2.2 Logical

This section contains the product features and denotes which are in the TOE.

1.5.2.2.1 Audit

The TOE generates audit records. The audit records can be displayed on the serial console as they are generated in a scrolling format.

The TOE writes audit logs to a text file stored in the systems flash memory for permanent storage. These audit log entries are tagged with the AOS Application that created them. The TOE also provides the ability to send switch logging information to an external syslog server using a secure channel.

The TOE provides to security administrators the ability to modify the maximum size allowed for the audit log files (the default value and allowed ranges for this value depends on the AOS version). Once the files are full the oldest entries are overwritten.

1.5.2.2.2 Administrator Identification and Authentication

Security Management is performed by administrators that must identify and authenticate to the TOE before any action. Whether through serial console or Secure Shell (SSH), the TOE requires the administrator to identify and authenticate to the TOE prior to accessing any of the management functionality. The TOE provides support for the following Identification and Authentication mechanisms:

- Identification and Authentication made by the TOE using credentials stored in the local file system;
- Identification and Authentication made by the TOE using credentials stored in a Lightweight Directory Access Protocol (LDAP) server, which is part of the operational environment; or
- Identification and Authentication made by an external authentication server, which is part of the operational environment.

The external authentication server supported by the TOE for administrator authentication is Remote Authentication Dial In User Service (RADIUS).

Communications with the RADIUS and LDAP servers can be protected with the Transport Layer Security (TLS) protocol.

The TOE provides administrator configurable password settings to enforce local password complexity when a password is created or modified. The TOE also displays to the user a configurable banner before a session starts, and provides the ability to terminate a session after a configurable period of inactivity.

1.5.2.2.3 Management of the TOE

The TOE provides the CLI for the TOE's security management functionality. The TOE also provides a Flash file system for storing configuration files/directories. Files can be transferred to the Flash file system via Secure File Transfer Protocol (SFTP).

The Simple Network Management Protocol (SNMP) is supported by the TOE but is not allowed in the evaluated configuration.

1.5.2.2.4 Cryptographic support

The TOE requires cryptography for supporting the following functionality.

- Establishment of secure channels using the SSHv2, TLSv1.1 and TLSv1.2 protocols
- X.509 certificate generation and validation
- Storage of passwords

The TOE provides cryptographic support using the OpenSSL and OpenSSH software packages, which are bundled in the TOE.

1.5.2.2.5 Protection of the TSF

The TOE protects itself by requiring administrators to identify and authenticate themselves prior to performing any actions and by defining the access allowed by each administrator. The TOE uses the filesystem access control to protect access to sensible data like cryptographic keys and credentials.

The TOE also implements self-tests to ensure the correct operation of cryptographic services, as well as integrity tests on software updates to ensure that software updates to the TOE can be trusted.

The TOE provides the following secure channels to ensure the integrity and confidentiality of the information exchanged between the TOE and external IT entities in the operational environment.

- Transport Layer Security (TLS) versions 1.1 and 1.2 are used to protect communication with authentication servers (RADIUS), LDAP servers, and audit servers (syslog).
- Secure Shell version 2 (SSHv2) is used to protect communication with SSH and SFTP clients and servers.

1.5.2.3 Non-Security Relevant TOE Features

The following table identifies other AOS features that are not security relevant and their usage does not impact the overall security of the product.

Feature	Description
LDAP Policy Server	LDAP Policy Server features are used to manage LDAP Policies. LDAP policies are QoS policies that are created via the PolicyView application and stored on an external LDAP server. The Policy Manager in the switch downloads these policies and keeps track of them. These policies cannot be modified directly on the switch. Since policies may only be modified via their originating source, LDAP policies must be modified through PolicyView and downloaded again to the switch.
Load balancing	Server Load Balancing (SLB) allows clients to send requests to servers logically grouped together in clusters. Each cluster logically aggregates a set of servers running identical applications with access to the same content (e.g., web servers). SLB uses a Virtual IP (VIP) address to treat a group of physical servers, each with a unique IP address, as one large virtual server. The switch will process requests by clients addressed to the VIP of the SLB cluster and send them to the physical servers. This process is totally transparent to the client.
Distance Vector Multicast Routing Protocol (DVMRP) / Protocol-Independent Multicast (PIM)	IP Multicast Routing Protocols
Spanning Tree	The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. Based on the IEEE 802.1D standard, the Alcatel STP implementation distributes the STP load between the primary management module and the network interface modules. In the case of a stack of switches, the STP load is distributed between the primary management switch and other switches in the stack.
Link Aggregation	Link aggregation allows you to combine two, four, or eight physical connections into large virtual connections known as link aggregation groups. You can configure VLANs, QoS conditions, 802.1Q framing, and other networking features on link aggregation groups because the switch's software treats these virtual links just like physical links.

Table 3: TOE functionality excluded from the TSF

1.5.2.4 Excluded TOE Features

The following features interfere with the TOE security functionality claims and must be disabled or not configured for use in the evaluated configuration.

Authenticated VLAN

(feature provided only in AOS 6.7.1.R04)

An authenticated VLAN grants end-users access to one or more VLANs after successful authentication at the switch port. Authenticated VLAN permissions are granted to end-users (not devices) leveraging external RADIUS, or LDAP directory servers, an authenticated VLAN grants end-users access to one or more VLANs after successful authentication at the switch port. Authenticated VLAN permissions are granted to end-users (not devices) leveraging external RADIUS, or LDAP directory servers.

This feature is superseded by Captive Portal and has been kept in the product for backwards compatibility reasons.

- Alcatel-Lucent-proprietary authentication client for VLAN-authentication
- Telnet authentication client for VLAN-authentication

Captive Portal

This feature allows web-based authentication of end-users.

Terminal Access Controller Access-Control System Plus (TACACS+)

Authentication using an external TACACS+ server is not allowed in the CC evaluated configuration.

Internetwork Packet Exchange (IPX) forwarding (routing)

(feature provided only in AOS 6.7.1.R04)

This feature has been kept in the product for backwards compatibility reasons.

Port Mobility Rules

Port mobility allows dynamic VLAN port assignment based on VLAN rules that are applied to port traffic.

This feature is superseded by User network profiles and has been kept in the product for backwards compatibility reasons.

FTP access to the switch

FTP traffic is not secured so the FTP service must be disabled for security reasons

Telnet access to the switch

Telnet traffic is not secured so the Telnet service must be disabled for security reasons.

Webview

This web-based interface used for switch management must be disabled.

Simple Network Management Protocol (SNMP)

SNMP must be disabled in the CC evaluated configuration.

Hypertext Transfer Protocol (HTTP)

HTTP and HTTPs must be disabled in the CC evaluated configuration.

Cryptographic algorithms

The MD5 algorithm cannot be used.

Network Time Protocol (NTP)

The use of NTP to synchronize the time with an external time source must be disabled in the CC evaluated configuration.

IPSec

IPSec must be disabled in the CC evaluated configuration.

1.5.2.5 Operational Environment

This section describes requirements on the environment in which the TOE is operated. The intended TOE environment is a secure data center that protects the TOE from unauthorized physical access. Only security administrators are to have access to connect to the serial console, or gain physical access to the hardware storing log data. Appropriate administrator security policy and security procedure guidance must be in place to govern operational management of the TOE within its operational environment.

- Versions 1.1 and 1.2 of the TLS protocol are the only versions allowed in the evaluated configuration. Usage of other protocol versions usually supported in SSL and TLS (SSLv1.0, SSLv2.0, SSLv3.0 or TLSv1.0) are prohibited.
- If the TOE is configured to use a RADIUS authentication server, or an LDAP server for credential storage, the TOE is dependent upon this external server in the operational environment for authentication.
- If the TOE is configured to use an LDAP server for credential storage, then a TLSv1.1 or TLSv1.2 capable LDAP server is required in the operational environment.
- If the TOE is configured to use a RADIUS external server for credential storage, then a TLSv1.1 or TLSv1.2 capable RADIUS server is required in the operational environment.
- If the TOE is configured to send switch logging output files (syslog files) to a remote IP address, a TLSv1.1 or TLSv1.2 capable syslog server is required in the operational environment.
- A serial console connected to the appliance must be available for installation and initial configuration. Once installation and configuration is completed, access to the TOE can be performed via the serial console as well as a remote console.
- If remote console is used, the Operational Environment must include an SSHv2 client.
- File transfers between the TOE and external servers, when the TOE is acting either as a client or a server, must be only performed using SFTP. FTP and Trivial File Transfer Protocol (TFTP) are forbidden. In this case, the Operational Environment must include an SFTP client or server.

2 CC Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 conformant.

This Security Target claims conformance to the following Protection Profiles and PP packages:

- [ND-cPPv1.0]☝: collaborative Protection Profile for Network Devices. Version 1.0 as of 2015-02-27; exact conformance.

Common Criteria [CC] version 3.1 revision 4 is the basis for this conformance claim.

3 Security Problem Definition

3.1 Threat Environment

This section describes the threat model for the TOE and identifies the individual threats that are assumed to exist in the TOE environment.

The **assets** to be protected by the TOE are as follows.

- Communications with the TOE: for administering the TOE (administration traffic), for sending and receiving authentication information sent to external servers (authentication traffic), and for sending audit records to an external audit server (audit traffic).
- The current version of the TOE and trusted updates to its firmware.
- TSF data stored by the TOE (e.g. user credentials, digital certificates).

The **threat agents** having an interest in manipulating the data model can be categorized as either:

- Unauthorized individuals (“attackers”) which are unknown to the TOE and its runtime environment.
- Authorized users of the TOE (i.e., administrators) who try to manipulate data that they are not authorized to access.

Threat agents originate from a well managed user community within an organizations internal network. Hence, only inadvertent or casual attempts to breach system security are expected from this community.

TOE administrators, including administrators of the TOE environment, are assumed to be trustworthy, trained and to follow the instructions provided to them with respect to the secure configuration and operation of the systems under their responsibility. Hence, only inadvertent attempts to manipulate the safe operation of the TOE are expected from this community.

3.1.1 Threats countered by the TOE

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents 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.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents 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

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints (e.g. a 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 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.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY

Threat agents 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.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents 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.PASSWORD_CRACKING

Threat agents 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_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.

3.2 Assumptions

3.2.1 Intended usage of the TOE

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).

3.2.2 Environment of use of the TOE

3.2.2.1 Physical

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's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.

3.2.2.2 Personnel

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. 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.

A.REGULAR_UPDATES

The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.ADMIN_CREDENTIALS_SECURE

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

3.2.2.3 Connectivity

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 Network Device collaborative Protection Profile ([ND-cPPv1.0]☝). It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).

3.3 Organizational Security Policies

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.

4 Security Objectives

4.1 Objectives for the TOE

This ST does not define security objectives for the TOE.

4.2 Objectives for 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.NO_GENERAL_PURPOSE

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.

OE.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

OE.UPDATES

The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

OE.ADMIN_CREDENTIALS_SECURE

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

OE.NO_THRU_TRAFFIC_PROTECTION

The 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.

4.3 Security Objectives Rationale

4.3.1 Coverage

This ST does not define security objectives for the TOE.

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.PHYSICAL	A.PHYSICAL_PROTECTION

Objective	Assumptions / Threats / OSPs
OE.NO_GENERAL_PURPOSE	A.LIMITED_FUNCTIONALITY
OE.TRUSTED_ADMIN	A.TRUSTED_ADMINISTRATOR
OE.UPDATES	A.REGULAR_UPDATES
OE.ADMIN_CREDENTIALS_SECURE	A.ADMIN_CREDENTIALS_SECURE
OE.NO_THRU_TRAFFIC_PROTECTION	A.NO_THRU_TRAFFIC_PROTECTION

Table 4: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

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

Threat	Rationale for security objectives
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	The [ND-cPPv1.0]☝ does not define security objectives.
T.WEAK_CRYPTOGRAPHY	The [ND-cPPv1.0]☝ does not define security objectives.
T.UNTRUSTED_COMMUNICATION_CHANNELS	The [ND-cPPv1.0]☝ does not define security objectives.
T.WEAK_AUTHENTICATION_ENDPOINTS	The [ND-cPPv1.0]☝ does not define security objectives.
T.UPDATE_COMPROMISE	The [ND-cPPv1.0]☝ does not define security objectives.
T.UNDETECTED_ACTIVITY	The [ND-cPPv1.0]☝ does not define security objectives.
T.SECURITY_FUNCTIONALITY_COMPROMISE	The [ND-cPPv1.0]☝ does not define security objectives.
T.PASSWORD_CRACKING	The [ND-cPPv1.0]☝ does not define security objectives.
T.SECURITY_FUNCTIONALITY_FAILURE	The [ND-cPPv1.0]☝ does not define security objectives.

Table 5: Sufficiency of objectives countering 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.LIMITED_FUNCTIONALITY	The assumption: ● 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). is upheld by: ● OE.NO_GENERAL_PURPOSE: 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	The assumption: ● 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's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. is upheld by: ● OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
A.TRUSTED_ADMINISTRATOR	The assumption: ● 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. 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. is upheld by: ● OE.TRUSTED_ADMIN: TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
A.REGULAR_UPDATES	The assumption: ● The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities. is upheld by: ● OE.UPDATES: The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The assumption:

Assumption	Rationale for security objectives
	- The administrator’s credentials (private key) used to access the network device are protected by the platform on which they reside. is upheld by: - OE.ADMIN_CREDENTIALS_SECURE: The administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
A.NO_THRU_TRAFFIC_PROTECTION	The assumption: - 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 ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall). is upheld by: - OE.NO_THRU_TRAFFIC_PROTECTION: The 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.

Table 6: Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy (OSP), that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented.

OSP	Rationale for security objectives
P.ACCESS_BANNER	The OSP: - 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. is enforced by: - FTA_TAB.1: Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

Table 7: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

The Security Target draws upon the extended components implicitly defined in the [ND-cPPv1.0]☝.

6 Security Requirements

6.1 TOE Security Functional Requirements

The Security Functional Requirements (SFRs) have been defined based on all SFRs included in [ND-cPPv1.0]☝, for which this ST claims exact conformance.

The following table shows the SFRs for the TOE, and the operations performed on the components according to CC part 1: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		ND-cPPv1.0	No	No	No	Yes
	FAU_GEN.2 User identity association		ND-cPPv1.0	No	No	No	No
	FAU_STG_EXT.1 Extended: Protected audit event storage		ND-cPPv1.0	No	No	Yes	Yes
	FAU_STG.1 Protected audit trail storage		ND-cPPv1.0	No	No	No	No
FCS - Cryptographic support	FCS_CKM.1 / AOS6.7.1 Cryptographic key generation (AOS6.7.1)	FCS_CKM.1	ND-cPPv1.0	Yes	No	No	Yes
	FCS_CKM.1 / AOS8.3.1 Cryptographic key generation (AOS8.3.1)	FCS_CKM.1	ND-cPPv1.0	Yes	Yes	No	Yes
	FCS_CKM.2 / AOS6.7.1 Cryptographic key distribution (AOS6.7.1)	FCS_CKM.2	ND-cPPv1.0	Yes	No	No	Yes
	FCS_CKM.2 / AOS8.3.1 Cryptographic key distribution (AOS8.3.1)	FCS_CKM.2	ND-cPPv1.0	Yes	No	No	Yes
	FCS_CKM.4 Cryptographic key destruction		ND-cPPv1.0	No	No	No	Yes
	FCS_COP.1(1) / AOS6.7.1 Cryptographic Operation (AES Data Encryption/Decryption) (AOS6.7.1)	FCS_COP.1	ND-cPPv1.0	Yes	No	No	Yes
	FCS_COP.1(1) / AOS8.3.1 Cryptographic Operation (AES Data Encryption/Decryption) (AOS8.3.1)	FCS_COP.1	ND-cPPv1.0	Yes	No	No	Yes
	FCS_COP.1(2) / AOS6.7.1 Cryptographic Operation (Signature Generation and Verification) (AOS6.7.1)	FCS_COP.1	ND-cPPv1.0	Yes	No	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FCS_COP.1(2) / AOS8.3.1 Cryptographic Operation (Signature Generation and Verification) (AOS8.3.1)	FCS_COP.1	ND-cPPv1.0	Yes	No	Yes	Yes
	FCS_COP.1(3) / AOS6.7.1 Cryptographic Operation (Hash Algorithm) (AOS6.7.1)	FCS_COP.1	ND-cPPv1.0	Yes	No	No	Yes
	FCS_COP.1(3) / AOS8.3.1 Cryptographic Operation (Hash Algorithm) (AOS8.3.1)	FCS_COP.1	ND-cPPv1.0	Yes	No	No	Yes
	FCS_COP.1(4) / AOS6.7.1 Cryptographic Operation (Keyed Hash Algorithm) (AOS6.7.1)	FCS_COP.1	ND-cPPv1.0	Yes	No	Yes	Yes
	FCS_COP.1(4) / AOS8.3.1 Cryptographic Operation (Keyed Hash Algorithm) (AOS8.3.1)	FCS_COP.1	ND-cPPv1.0	Yes	No	Yes	Yes
	FCS_RBG_EXT.1 Extended: Random bit generation		ND-cPPv1.0	No	No	Yes	Yes
	FCS_SSHC_EXT.1 / AOS6.7.1 Extended: SSH Client Protocol (AOS6.7.1)	FCS_SSHC_EXT.1	ND-cPPv1.0	Yes	No	Yes	Yes
	FCS_SSHC_EXT.1 / AOS8.3.1 Extended: SSH Client Protocol (AOS8.3.1)	FCS_SSHC_EXT.1	ND-cPPv1.0	Yes	No	Yes	Yes
	FCS_SSHS_EXT.1 / AOS6.7.1 Extended: SSH Server Protocol (AOS6.7.1)	FCS_SSHS_EXT.1	ND-cPPv1.0	Yes	No	Yes	Yes
	FCS_SSHS_EXT.1 / AOS8.3.1 Extended: SSH Server Protocol (AOS8.3.1)	FCS_SSHS_EXT.1	ND-cPPv1.0	Yes	No	Yes	Yes
	FCS_TLSC_EXT.2 / AOS6.7.1 Extended: TLS Client Protocol with authentication (AOS6.7.1)	FCS_TLSC_EXT.2	ND-cPPv1.0	Yes	No	No	Yes
	FCS_TLSC_EXT.2 / AOS8.3.1 Extended: TLS Client Protocol with authentication (AOS8.3.1)	FCS_TLSC_EXT.2	ND-cPPv1.0	Yes	No	No	Yes
FIA - Identification and authentication	FIA_PMG_EXT.1 Extended: Password management		ND-cPPv1.0	No	No	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FIA_UIA_EXT.1 Extended: Identification and authentication		ND-cPPv1.0	No	No	No	Yes
	FIA_UAU_EXT.2 Extended: Password-based authentication mechanism		ND-cPPv1.0	No	No	No	Yes
	FIA_UAU.7 Protected authentication feedback		ND-cPPv1.0	No	No	No	No
	FIA_X509_EXT.1 Extended: X.509 certificate validation		ND-cPPv1.0	No	No	No	Yes
	FIA_X509_EXT.2 Extended: X.509 certificate authentication		ND-cPPv1.0	No	No	No	Yes
	FIA_X509_EXT.3 Extended: X.509 certificate requests		ND-cPPv1.0	No	No	No	Yes
FMT - Security management	FMT_MOF.1(1) / TrustedUpdate Management of security functions behaviour (Trusted Updates)	FMT_MOF.1	ND-cPPv1.0	Yes	No	No	No
	FMT_MTD.1 Management of TSF data		ND-cPPv1.0	No	No	No	No
	FMT_SMF.1 Specification of management functions		ND-cPPv1.0	No	No	No	Yes
	FMT_SMR.2 Restrictions on security roles		ND-cPPv1.0	No	No	No	No
	FMT_MOF.1(1) / Audit Management of security functions behaviour	FMT_MOF.1	ND-cPPv1.0	Yes	No	No	No
	FMT_MOF.1(2) / Audit Management of security functions behaviour	FMT_MOF.1	ND-cPPv1.0	Yes	No	No	No
	FMT_MOF.1(1) / AdminAct Management of security functions behaviour	FMT_MOF.1	ND-cPPv1.0	Yes	No	No	No
	FMT_MTD.1 / AdminAct Management of TSF Data	FMT_MTD.1	ND-cPPv1.0	Yes	No	No	No
FPT - Protection of the TSF	FPT_SKP_EXT.1 Extended: Protection of TSF data (for reading of all symmetric keys)		ND-cPPv1.0	No	No	No	No
	FPT_APW_EXT.1 Extended: Protection of administrator passwords		ND-cPPv1.0	No	No	No	No

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FPT_TST_EXT.1 Extended: TSF testing		ND-cPPv1.0	No	No	Yes	Yes
	FPT_TUD_EXT.1 Extended: Trusted update		ND-cPPv1.0	No	No	No	Yes
	FPT_STM.1 Reliable time stamps		ND-cPPv1.0	No	No	No	No
FTA - TOE access	FTA_SSL_EXT.1 Extended: TSF-initiated session locking		ND-cPPv1.0	No	No	No	Yes
	FTA_SSL.3 TSF-initiated termination		ND-cPPv1.0	No	No	No	No
	FTA_SSL.4 User-initiated termination		ND-cPPv1.0	No	No	No	No
	FTA_TAB.1 Default TOE access banners		ND-cPPv1.0	No	No	No	No
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		ND-cPPv1.0	No	Yes	Yes	Yes
	FTP_TRP.1 Trusted path		ND-cPPv1.0	No	No	No	Yes

Table 8: SFRs for the TOE

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

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) 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).
- Starting and stopping services (if applicable)
- **no other actions**

d) Specifically defined auditable events listed in Table 9.

Application Note: *The term "services" refers to trusted path and trusted channel communications and administrator sessions.*

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column three of Table 9.

Requirement	**Auditable Events**	**Additional Audit Record Contents**
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_STG_EXT.1	None	None
FCS_CKM.1 / AOS6.7.1, FCS_CKM.1 / AOS8.3.1	None	None
FCS_CKM.2 / AOS6.7.1, FCS_CKM.2 / AOS8.3.1	None	None
FCS_CKM.4	None	None
FCS_COP.1(1) / AOS6.7.1, FCS_COP.1(1) / AOS8.3.1	None	None
FCS_COP.1(2) / AOS6.7.1, FCS_COP.1(2) / AOS8.3.1	None	None
FCS_COP.1(3) / AOS6.7.1, FCS_COP.1(3) / AOS8.3.1	None	None
FCS_COP.1(4) / AOS6.7.1, FCS_COP.1(4) / AOS8.3.1	None	None
FCS_RBG_EXT.1	None	None
FIA_PMG_EXT.1	None	None
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Provided user identity, origin of the attempt (only for SSHv2 connections)
FIA_UAU_EXT.2	All use of the identification and authentication mechanism	Origin of the attempt (only for SSHv2 connections).
FIA_UAU.7	None	None
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None	None

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MOF.1(1) / TrustedUpdate	Any attempt to initiate a manual update	None
FMT_MTD.1	All management activities of TSF data	None
FMT_SMF.1	None	None
FMT_SMR.2	None	None
FPT_SKP_EXT.1	None	None
FPT_APW_EXT.1	None	None
FPT_TST_EXT.1	None	None
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	No additional information
FPT_STM.1	Changes to the time	Old and new time values
FTA_SSL_EXT.1	Termination of a local interactive session	None
FTA_SSL.3	Termination of a remote interactive session	None
FTA_SSL.4	The termination of an interactive session	None
FTA_TAB.1	None	None
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions	Identification of the claimed user identity
FAU_STG.1	None	None
FMT_MOF.1(1) / Audit	Modification of the behaviour of the transmission of audit data to an external IT entity	None
FMT_MOF.1(2) / Audit	Modification of the behaviour of the handling of audit data	None
FMT_MOF.1(1) / AdminAct	Modification of the behaviour of the TSF	None
FMT_MTD.1 / AdminAct	Modification, deletion, generation/import of cryptographic keys	None
FCS_SSHC_EXT.1 / AOS6.7.1, FCS_SSHC_EXT.1 / AOS8.3.1	Failure to establish an SSH session	Reason for failure

Requirement	Auditable Events	Additional Audit Record Contents
Non-TOE endpoint of connection (IP Address)		
FCS_SSHS_EXT.1 / AOS6.7.1, FCS_SSHS_EXT.1 / AOS8.3.1	Failure to establish an SSH session	Reason for failure
Non-TOE endpoint of connection (IP Address)		
FCS_TLSC_EXT.2 / AOS6.7.1, FCS_TLSC_EXT.2 / AOS8.3.1	Failure to establish an TLS Session	Reason for failure

Table 9: Security Functional Requirements and Auditable Events

6.1.1.2 User identity association (FAU_GEN.2)

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

6.1.1.3 Extended: Protected audit event storage (FAU_STG_EXT.1)

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

FAU_STG_EXT.1.3 The TSF shall **overwrite previous audit records according to the following rule: overwrite the data present in the oldest audit file** when the local storage space for audit data is full.

6.1.1.4 Protected audit trail storage (FAU_STG.1)

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

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

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation (AOS6.7.1) (FCS_CKM.1 / AOS6.7.1)

FCS_CKM.1.1 / AOS6.7.1 The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm:

- **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;**

6.1.2.2 Cryptographic key generation (AOS8.3.1) (FCS_CKM.1 / AOS8.3.1)

FCS_CKM.1.1 / AOS8.3.1 The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm:

- **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;**
- **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;**

6.1.2.3 Cryptographic key distribution (AOS6.7.1) (FCS_CKM.2 / AOS6.7.1)

FCS_CKM.2.1 / AOS6.7.1 The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

- **RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”;**

6.1.2.4 Cryptographic key distribution (AOS8.3.1) (FCS_CKM.2 / AOS8.3.1)

FCS_CKM.2.1 / AOS8.3.1 The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

- **RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”;**
- **Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;**

6.1.2.5 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- For plaintext keys in volatile storage, the destruction shall be executed by a **single overwrite consisting of zeroes**;
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that
  - **instructs a part of the TSF to destroy the abstraction that represents the key**

that meets the following: No Standard.

6.1.2.6 Cryptographic Operation (AES Data Encryption/Decryption) (AOS6.7.1) (FCS_COP.1(1) / AOS6.7.1)

FCS_COP.1.1(1) / AOS6.7.1 The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in **CBC** mode and cryptographic key sizes **128 bits, 256 bits** that meet the following: AES as specified in ISO 18033-3, **CBC as specified in ISO 10116**.

6.1.2.7 Cryptographic Operation (AES Data Encryption/Decryption) (AOS8.3.1) (FCS_COP.1(1) / AOS8.3.1)

FCS_COP.1.1(1) / AOS8.3.1 The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in **CBC, GCM** mode and cryptographic key sizes **128 bits, 256 bits** that meet the following: AES as specified in ISO 18033-3, **CBC as specified in ISO 10116, GCM as specified in ISO 19772**.

6.1.2.8 Cryptographic Operation (Signature Generation and Verification) (AOS6.7.1) (FCS_COP.1(2) / AOS6.7.1)

FCS_COP.1.1(2) / AOS6.7.1 The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm

- **RSA Digital Signature Algorithm and cryptographic key sizes (modulus) 2048 bits**

that meet the following:

- **For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,**

.

6.1.2.9 Cryptographic Operation (Signature Generation and Verification) (AOS8.3.1) (FCS_COP.1(2) / AOS8.3.1)

FCS_COP.1.1(2) / AOS8.3.1 The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm

- **RSA Digital Signature Algorithm and cryptographic key sizes (modulus) 2048 bits**
- **Elliptic Curve Digital Signature Algorithm and cryptographic key sizes 256 bits, 384 bits and 521 bits**

that meet the following:

- **For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,**
- **For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, and P-521; ISO/IEC 14888-3, Section 6.4**

.

6.1.2.10 Cryptographic Operation (Hash Algorithm) (AOS6.7.1) (FCS_COP.1(3) / AOS6.7.1)

FCS_COP.1.1(3) / AOS6.7.1 The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm **SHA-1, SHA-256** that meet the following: ISO/IEC 10118-3:2004.

6.1.2.11 Cryptographic Operation (Hash Algorithm) (AOS8.3.1) (FCS_COP.1(3) / AOS8.3.1)

FCS_COP.1.1(3) / AOS8.3.1 The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm **SHA-1, SHA-256, SHA-384, SHA-512** that meet the following: ISO/IEC 10118-3:2004.

6.1.2.12 Cryptographic Operation (Keyed Hash Algorithm) (AOS6.7.1) (FCS_COP.1(4) / AOS6.7.1)

FCS_COP.1.1(4) / AOS6.7.1 The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm **HMAC-SHA-1, HMAC-SHA-256** and cryptographic key sizes **256 bits** and message digest sizes **160, 256** bits that meets ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.

6.1.2.13 Cryptographic Operation (Keyed Hash Algorithm) (AOS8.3.1) (FCS_COP.1(4) / AOS8.3.1)

FCS_COP.1.1(4) / AOS8.3.1 The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm **HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512** and cryptographic key sizes **256 bits** and message digest sizes **160, 256, 384, 512** bits that meets ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.

6.1.2.14 Extended: Random bit generation (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using **Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)**.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from **a single software-based noise source** with a minimum of **256 bits** of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

6.1.2.15 Extended: SSH Client Protocol (AOS6.7.1) (FCS_SSHC_EXT.1 / AOS6.7.1)

FCS_SSHC_EXT.1.1 / AOS6.7.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and **no other RFCs**.

FCS_SSHC_EXT.1.2 / AOS6.7.1 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in [RFC4252]☝: public key-based, password-based.

FCS_SSHC_EXT.1.3 / AOS6.7.1 The TSF shall ensure that, as described in [RFC4253], packets greater than **256K** bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4 / AOS6.7.1 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: aes128-cbc, aes256-cbc, **no other algorithms**.

FCS_SSHC_EXT.1.5 / AOS6.7.1 The TSF shall ensure that the SSH transport implementation uses **ssh-rsa** and **no other public key algorithms** as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6 / AOS6.7.1 The TSF shall ensure that the SSH transport implementation uses **hmac-sha1, hmac-sha1-96, hmac-sha2-256** and **no other MAC algorithms** as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7 / AOS6.7.1 TSF shall ensure that **diffie-hellman-group14-sha1** and **no other methods** are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8 / AOS6.7.1 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^28 packets have been transmitted using that key.

FCS_SSHC_EXT.1.9 / AOS6.7.1 The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key or **no other methods** as described in [RFC4251] section 4.1.

6.1.2.16 Extended: SSH Client Protocol (AOS8.3.1) (FCS_SSHC_EXT.1 / AOS8.3.1)

FCS_SSHC_EXT.1.1 / AOS8.3.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and **5656, 6668, no other RFCs**.

FCS_SSHC_EXT.1.2 / AOS8.3.1 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in [RFC4252]: public key-based, password-based.

FCS_SSHC_EXT.1.3 / AOS8.3.1 The TSF shall ensure that, as described in [RFC4253], packets greater than **256K** bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4 / AOS8.3.1 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: aes128-cbc, aes256-cbc, **no other algorithms**.

FCS_SSHC_EXT.1.5 / AOS8.3.1 The TSF shall ensure that the SSH transport implementation uses **ssh-rsa, ecdsa-sha2-nistp256** and **no other public key algorithms** as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6 / AOS8.3.1 The TSF shall ensure that the SSH transport implementation uses **hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512** and **no other MAC algorithms** as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7 / AOS8.3.1 TSF shall ensure that **diffie-hellman-group14-sha1, ecdh-sha2-nistp256** and **ecdh-sha2-nistp384, ecdh-sha2-nistp521** are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8 / AOS8.3.1 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^28 packets have been transmitted using that key.

FCS_SSHC_EXT.1.9 / AOS8.3.1 The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key or **no other methods** as described in [RFC4251] section 4.1.

6.1.2.17 Extended: SSH Server Protocol (AOS6.7.1) (FCS_SSHS_EXT.1 / AOS6.7.1)

FCS_SSHS_EXT.1.1 / AOS6.7.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and **no other RFCs**.

FCS_SSHS_EXT.1.2 / AOS6.7.1 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in [RFC4252]☝: public key-based, password-based.

FCS_SSHS_EXT.1.3 / AOS6.7.1 The TSF shall ensure that, as described in [RFC4253]☝, packets greater than **256K** bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 / AOS6.7.1 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: aes128-cbc, aes256-cbc, **no other algorithms**.

FCS_SSHS_EXT.1.5 / AOS6.7.1 The TSF shall ensure that the SSH transport implementation uses **ssh-rsa** and **no other public key algorithms** as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 / AOS6.7.1 The TSF shall ensure that the SSH transport implementation uses **hmac-sha1, hmac-sha1-96, hmac-sha2-256** and **no other MAC algorithms** as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 / AOS6.7.1 TSF shall ensure that **diffie-hellman-group14-sha1** and **no other methods** are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 / AOS6.7.1 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^28 packets have been transmitted using that key.

6.1.2.18 Extended: SSH Server Protocol (AOS8.3.1) (FCS_SSHS_EXT.1 / AOS8.3.1)

FCS_SSHS_EXT.1.1 / AOS8.3.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and **5656, 6668, no other RFCs**.

FCS_SSHS_EXT.1.2 / AOS8.3.1 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in [RFC4252]☝: public key-based, password-based.

FCS_SSHS_EXT.1.3 / AOS8.3.1 The TSF shall ensure that, as described in [RFC4253]☝, packets greater than **256K** bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 / AOS8.3.1 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: aes128-cbc, aes256-cbc, **no other algorithms**.

FCS_SSHS_EXT.1.5 / AOS8.3.1 The TSF shall ensure that the SSH transport implementation uses **ssh-rsa, ecdsa-sha2-nistp256** and **no other public key algorithms** as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 / AOS8.3.1 The TSF shall ensure that the SSH transport implementation uses **hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512** and **no other MAC algorithms** as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 / AOS8.3.1 TSF shall ensure that **diffie-hellman-group14-sha1, ecdh-sha2-nistp256** and **ecdh-sha2-nistp384, ecdh-sha2-nistp521** are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 / AOS8.3.1 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^28 packets have been transmitted using that key.

6.1.2.19 Extended: TLS Client Protocol with authentication (AOS6.7.1) (FCS_TLSC_EXT.2 / AOS6.7.1)

FCS_TLSC_EXT.2.1 / AOS6.7.1 The TSF shall implement **TLS 1.1 ([RFC4346]), TLS 1.2 ([RFC5246])** supporting the following ciphersuites:

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA as defined in [RFC3268]
- Optional Ciphersuites:
  - **TLS_RSA_WITH_AES_256_CBC_SHA as defined in [RFC3268]**
  - **TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5246]**
  - **TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in [RFC5246]**

.

FCS_TLSC_EXT.2.2 / AOS6.7.1 The TSF shall verify that the presented identifier matches the reference identifier according to [RFC6125].

FCS_TLSC_EXT.2.3 / AOS6.7.1 The TSF shall only establish a trusted channel if the peer certificate is valid.

FCS_TLSC_EXT.2.4 / AOS6.7.1 The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: **none** and no other curves.

FCS_TLSC_EXT.2.5 / AOS6.7.1 The TSF shall support mutual authentication using X.509v3 certificates.

6.1.2.20 Extended: TLS Client Protocol with authentication (AOS8.3.1) (FCS_TLSC_EXT.2 / AOS8.3.1)

FCS_TLSC_EXT.2.1 / AOS8.3.1 The TSF shall implement **TLS 1.1 ([RFC4346]), TLS 1.2 ([RFC5246])** supporting the following ciphersuites:

- Mandatory Ciphersuites:
  - TLS_RSA_WITH_AES_128_CBC_SHA as defined in [RFC3268]
- Optional Ciphersuites:
  - **TLS_RSA_WITH_AES_256_CBC_SHA as defined in [RFC3268]**
  - **TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in [RFC3268]**
  - **TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in [RFC3268]**
  - **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in [RFC4492]**
  - **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in [RFC4492]**
  - **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in [RFC4492]**
  - **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in [RFC4492]**
  - **TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5246]**
  - **TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in [RFC5246]**

- ○ **TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5246]**☝
- ○ **TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in [RFC5246]**☝
- ○ **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in [RFC5289]**☝
- ○ **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in [RFC5289]**☝
- ○ **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in [RFC5289]**☝
- ○ **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in [RFC5289]**☝
- ○ **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in [RFC5289]**☝
- ○ **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in [RFC5289]**☝

.

FCS_TLSC_EXT.2.2 / AOS8.3.1 The TSF shall verify that the presented identifier matches the reference identifier according to [RFC6125]☝.

FCS_TLSC_EXT.2.3 / AOS8.3.1 The TSF shall only establish a trusted channel if the peer certificate is valid.

FCS_TLSC_EXT.2.4 / AOS8.3.1 The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: **secp256r1, secp384r1, secp521r1** and no other curves.

FCS_TLSC_EXT.2.5 / AOS8.3.1 The TSF shall support mutual authentication using X.509v3 certificates.

6.1.3 Identification and authentication (FIA)

6.1.3.1 Extended: Password management (FIA_PMG_EXT.1)

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: **"@", "#", "$", "%", "^", "&", "*", "(", ")", “~”, “{“, “}”, “[“, ”]”, “:”, “;”, “|“, “\“, “/”, “.”, “<” and “>";**

b) Minimum password length shall be settable by the Security Administrator, and shall support passwords of 15 characters or greater.

6.1.3.2 Extended: Identification and authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- **no other actions**

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

6.1.3.3 Extended: Password-based authentication mechanism (FIA_UAU_EXT.2)

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, **none** to perform administrative user authentication.

6.1.3.4 Protected authentication feedback (FIA_UAU.7)

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

6.1.3.5 Extended: X.509 certificate validation (FIA_X509_EXT.1)

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- [RFC5280]☝ certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using **the Online Certificate Status Protocol (OCSP) as specified in [RFC2560]☝, a Certificate Revocation List (CRL) as specified in [RFC5759]☝**.
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

Application Note: *The TOE validates a certificate using the CRL stored in the flash filesystem. The TOE does not have the capability of downloading CRLs.*

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

6.1.3.6 Extended: X.509 certificate authentication (FIA_X509_EXT.2)

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by [RFC5280] to support authentication for **TLS** and **no additional uses.**

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall **not accept the certificate**.

Application Note: *Certificate revocation is verified by using an OCSP server and CRLs.*

6.1.3.7 Extended: X.509 certificate requests (FIA_X509_EXT.3)

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request Message as specified by [RFC2986] and be able to provide the following information in the request: public key and **Common Name, Organization, Organizational Unit, Country**.

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

6.1.4 Security management (FMT)

6.1.4.1 Management of security functions behaviour (Trusted Updates) (FMT_MOF.1(1) / TrustedUpdate)

FMT_MOF.1.1(1) / TrustedUpdate The TSF shall restrict the ability to enable the functions to perform manual update to Security Administrators.

6.1.4.2 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to manage the TSF data to Security Administrators.

6.1.4.3 Specification of management functions (FMT_SMF.1)

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

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using **hash comparison** capability prior to installing those updates;
- **Ability to configure audit behavior;**

6.1.4.4 Restrictions on security roles (FMT_SMR.2)

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

a) The Security Administrator role shall be able to administer the TOE locally;

b) The Security Administrator role shall be able to administer the TOE remotely are satisfied.

6.1.4.5 Management of security functions behaviour (FMT_MOF.1(1) / Audit)

FMT_MOF1.1(1) / Audit The TSF shall restrict the ability to determine the behaviour of, modify the behaviour of the functions transmission of audit data to an external IT entity to Security Administrators.

6.1.4.6 Management of security functions behaviour (FMT_MOF.1(2) / Audit)

FMT_MOF.1.1(2) / Audit The TSF shall restrict the ability to determine the behaviour of, modify the behaviour of the functions handling of audit data to Security Administrators.

6.1.4.7 Management of security functions behaviour (FMT_MOF.1(1) / AdminAct)

FMT_MOF.1.1(1) / AdminAct The TSF shall restrict the ability to modify the behaviour of the functions TOE Security Functions to Security Administrators

6.1.4.8 Management of TSF Data (FMT_MTD.1 / AdminAct)

FMT_MTD.1.1 / AdminAct The TSF shall restrict the ability to modify, delete, generate/import the cryptographic keys to Security Administrators.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 Extended: Protection of TSF data (for reading of all symmetric keys) (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.1.5.2 Extended: Protection of administrator passwords (FPT_APW_EXT.1)

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.

6.1.5.3 Extended: TSF testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests **during initial start-up (on power on), at the conditions none** to demonstrate the correct operation of the TSF: **power on self-tests required by the FIPS 140-2 standard in the OpenSSL cryptographic module**.

6.1.5.4 Extended: Trusted update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1 The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and **the most recently installed version of the TOE firmware/software**.

FPT_TUD_EXT.1.2 The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and **no other update mechanism**.

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a **published hash** prior to installing those updates.

6.1.5.5 Reliable time stamps (FPT_STM.1)

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

6.1.6 TOE access (FTA)

6.1.6.1 Extended: TSF-initiated session locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions,

- **terminate the session**

after a Security Administrator-specified time period of inactivity.

6.1.6.2 TSF-initiated termination (FTA_SSL.3)

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

Application note: *This requirement is applicable to sessions regardless of whether the user has been already authenticated successfully or not (login prompt).*

6.1.6.3 User-initiated termination (FTA_SSL.4)

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

6.1.6.4 Default TOE access banners (FTA_TAB.1)

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

6.1.7 Trusted path/channels (FTP)

6.1.7.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall be capable of using **SSH, TLS** to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, ***RADIUS*** **authentication server, LDAP server, SSH**

server, SFTP server that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **sending audit records to the external syslog server, requesting user credentials to an LDAP server, requesting user authentication to a RADIUS authentication server, sending SSH and SFTP requests**.

Application Note: *The SSHv2 protocol is used for the SSH client, SSH server, SFTP client and SFTP server. TLSv1.1 and TLSv1.2 are used for protecting the communication with the RADIUS, LDAP and syslog external servers.*

6.1.7.2 Trusted path (FTP_TRP.1)

FTP_TRP.1.1 The TSF shall be capable of using **SSH** to provide a communication path between itself and authorized remote 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 administrators to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

This ST does not define security objectives for the TOE.

6.2.2 Sufficiency

This ST does not define security objectives for the TOE.

6.2.3 Security Requirements Dependency Analysis

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	FAU_GEN.1
	FIA_UID.1	FIA_UIA_EXT.1

Security functional requirement	Dependencies	Resolution
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1
	FTP_ITC.1	FTP_ITC.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1 / AOS6.7.1	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1(2) / AOS6.7.1
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.1 / AOS8.3.1	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1(2) / AOS8.3.1
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.2 / AOS6.7.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 / AOS6.7.1
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.2 / AOS8.3.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 / AOS8.3.1
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 / AOS6.7.1 FCS_CKM.1 / AOS8.3.1
FCS_COP.1(1) / AOS6.7.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 / AOS6.7.1
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1(1) / AOS8.3.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 / AOS8.3.1
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1(2) / AOS6.7.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 / AOS6.7.1
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1(2) / AOS8.3.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 / AOS8.3.1
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1(3) / AOS6.7.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Unresolved dependency because keys are not required for the hashing algorithms defined in FCS_COP.1(3) / AOS6.7.1
	FCS_CKM.4	Unresolved dependency because keys are not required for the hashing algorithms defined in FCS_COP.1(3) / AOS6.7.1
FCS_COP.1(3) / AOS8.3.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Unresolved dependency because keys are not required for the hashing algorithms defined in FCS_COP.1(3) / AOS8.3.1
	FCS_CKM.4	Unresolved dependency because keys are not required for the hashing algorithms defined in FCS_COP.1(3) / AOS8.3.1

Security functional requirement	Dependencies	Resolution
FCS_COP.1(4) / AOS6.7.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 / AOS6.7.1
	FCS_CKM.4	FCS_CKM.4
FCS_COP.1(4) / AOS8.3.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 / AOS8.3.1
	FCS_CKM.4	FCS_CKM.4
FCS_RBG_EXT.1	No dependencies	
FCS_SSHC_EXT.1 / AOS6.7.1	FCS_COP.1	FCS_COP.1(1) / AOS6.7.1 FCS_COP.1(2) / AOS6.7.1 FCS_COP.1(3) / AOS6.7.1
FCS_SSHC_EXT.1 / AOS8.3.1	FCS_COP.1	FCS_COP.1(1) / AOS8.3.1 FCS_COP.1(2) / AOS8.3.1 FCS_COP.1(3) / AOS8.3.1
FCS_SSHS_EXT.1 / AOS6.7.1	FCS_COP.1	FCS_COP.1(1) / AOS6.7.1 FCS_COP.1(2) / AOS6.7.1 FCS_COP.1(3) / AOS6.7.1
FCS_SSHS_EXT.1 / AOS8.3.1	FCS_COP.1	FCS_COP.1(1) / AOS8.3.1 FCS_COP.1(2) / AOS8.3.1 FCS_COP.1(3) / AOS8.3.1
FCS_TLSC_EXT.2 / AOS6.7.1	FCS_COP.1	FCS_COP.1(1) / AOS6.7.1 FCS_COP.1(2) / AOS6.7.1 FCS_COP.1(3) / AOS6.7.1
	FCS_RBG_EXT.1	FCS_RBG_EXT.1
FCS_TLSC_EXT.2 / AOS8.3.1	FCS_COP.1	FCS_COP.1(1) / AOS8.3.1 FCS_COP.1(2) / AOS8.3.1 FCS_COP.1(3) / AOS8.3.1
	FCS_RBG_EXT.1	FCS_RBG_EXT.1
FIA_PMG_EXT.1	No dependencies	
FIA_UIA_EXT.1	FTA_TAB.1	FTA_TAB.1
FIA_UAU_EXT.2	No dependencies	
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1
FIA_X509_EXT.1	No dependencies	
FIA_X509_EXT.2	No dependencies	
FIA_X509_EXT.3	No dependencies	
FMT_MOF.1(1) / TrustedUpdate	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1

Security functional requirement	Dependencies	Resolution
FMT_MTD.1	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies	
FMT_SMR.2	FIA_UID.1	FIA_UIA_EXT.1
FMT_MOF.1(1) / Audit	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MOF.1(2) / Audit	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MOF.1(1) / AdminAct	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1 / AdminAct	FMT_SMR.1	FMT_SMR.2
	FMT_SMF.1	FMT_SMF.1
FPT_SKP_EXT.1	No dependencies	
FPT_APW_EXT.1	No dependencies	
FPT_TST_EXT.1	No dependencies	
FPT_TUD_EXT.1	FCS_COP.1	FCS_COP.1(3) / AOS6.7.1 FCS_COP.1(3) / AOS8.3.1
FPT_STM.1	No dependencies	
FTA_SSL_EXT.1	FIA_UAU.1	FIA_UIA_EXT.1
FTA_SSL.3	No dependencies	
FTA_SSL.4	No dependencies	
FTA_TAB.1	No dependencies	
FTP_ITC.1	No dependencies	
FTP_TRP.1	No dependencies	

Table 10: TOE SFR dependency analysis

6.2.4 Internal consistency and mutual support of SFRs

6.3 Security Assurance Requirements

The security assurance requirements (SARs) for the TOE are the components defined in the evaluation assurance package ND-cPPv1.0.

The following table shows the SARs, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	**Security assurance requirement**	**Source**	**Operations**			
			Iter.	**Ref.**	**Ass.**	**Sel.**
ASE Security Target evaluation	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_OBJ.1 Security objectives for the operational environment	CC Part 3	No	No	No	No
	ASE_REQ.1 Stated security requirements	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ADV Development	ADV_FSP.1 Basic functional specification	CC Part 3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.1 Labelling of the TOE	CC Part 3	No	No	No	No
	ALC_CMS.1 TOE CM coverage	CC Part 3	No	No	No	No
ATE Tests	ATE_IND.1 Independent testing - conformance	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.1 Vulnerability survey	CC Part 3	No	No	No	No

Table 11: SARs

6.4 Security Assurance Requirements Rationale

The [ND-cPPv1.0]☝ specifies the security assurance requirements (SARs) individually. Any and all rationale for this protection profile's selection of SARs is provided by the protection profile. No modifications and no augmentations have been made to the protection profile's SARs.

7 TOE Summary Specification

7.1 TOE Security Functionality

As per the [ND-cPPv1.0]☝, the TOE supports the following major security features.

- Auditing
- Cryptographic Support
- Identification and Authentication of TOE Administrators
- Security Management
- Protection of the TSF

7.1.1 Auditing

Audit functionality is provided via the Switch Logging feature, which records audit events for all administrative operations performed. Each audit record contains the date and time of the event, type of event, subject identity and outcome (success or failure). The type of event and outcome are included in the Log Message field which specifies the condition recorded.

The switch logging utility is the event logging application that supports the audit functionality in the TOE. The utility supports the severity levels detailed in Table 12.

Security Level	Type	Description
2 *(highest severity)*	Alarm	A serious, non-recoverable error has occurred and the system must be rebooted.
3	Error	System functionality is reduced.
4	Alert	A violation has occurred.
5	Warning	A unexpected, non-critical event has occurred.
6 *(default)*	Info	Any other non-debug message.
7	Debug1	A normal event debug message.
8	Debug2	A debug-specific message.
9 *(lowest severity)*	Debug3	A maximum verbosity debug message.

Table 12: TOE audit record levels

Specific security and administrative events that are required to be audited by this ST are labeled as "EVENT-AUDIT", and generated with security level 6 (Info). It is possible to configure the severity level either globally for all applications or on a per application basis. Security level 6 (Info) is enabled for all events by default and is the minimum severity level required in the evaluated configuration.

When an audit event request is made, the severity level on the request is compared to the severity level assigned to the application ID for which the event occurs. If the severity level of the log request is less than or equal to that of the application ID, the log message is generated and placed in the log file.

The switch logging utility can be configured to send audit records to a log file on the switch’s flash file system, display them on the serial console, and/or send them to a remote syslog server.

For local permanent storage, audit data is stored in an SWLOG file located in the flash file system. Whenever the audit file reaches the maximum size allowed, the audit file is backed up onto a set of circular audit files, discarding the oldest file. The amount of audit data that can be generated depends on the maximum size allowed for each of the audit log files, which can be changed using the command: **`swlog output flash file-size <size in KB>`**. The TOE also provides a mechanism to display a warning to the user if the storage capacity has reached 90% of the configured size in any of the SWLOG files.

In virtual chassis configurations (AOS 8.3.1.R01) a separate audit log set is generated for each chassis, CMM slot and NI slot that comprises the virtual chassis.

SWLOG files are protected from modification and deletion by enforcing access control on groups of commands. Only the Security Administrator has privileges to clear the audit logs.

The following table shows, for each AOS, the number of circular files that comprise the audit file set, the file names for the audit file set, the parameter used to define the maximum size allowed for audit records, and the default value and allowed range for that parameter.

Operating System	Number of circular files	Audit file set	Parameter definition	Default value	Allowed values
AOS 6.7.1.R04	Two	swlog1.log, swlog2.log	Maximum size for the set (in KB)	64KB	32KB up to space available in flash memory
AOS 8.3.1.R01	Eight	swlog_<suffix>[1], swlog_<suffix>.0 through swlog_*<suffix>.6	Maximum size for each file (in KB)	1250KB	125KB to 12500KB

Table 13: Audit permanent storage

The switch logging utility can also transfer audit data to an external syslog server. A secure communication channel is established between the TOE and the external syslog server using TLSv1.1 or TLSv1.2 in order to protect audit data communication from loss of integrity or confidentiality.

An audit record is sent to the remote server immediately after the event occurs. If communication fails with the syslog server, the audit event is only recorded locally and is not resent; the switch logging utility tries to reconnect to the syslog server whenever a new audit generation request is received.

7.1.1.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FAU_GEN.1
The audit functionality generates records for the auditable events specified in this SFR, including the general information required as well as the specific information required for each event.

FAU_GEN.2
Whenever possible, the audit functionality includes the user id that caused the event (some of the audit events do not have a user associated, e.g. failure in establishing a TLS session).

[1] this suffix depends on the Omniswitch model and the components that comprise the virtual chassis.

FAU_STG_EXT.1

Audit events are stored locally in the flash memory using a circular chain of audit files. When the audit file reaches a configurable threshold, the audit file is renamed, older audit files are shifted, and if the oldest audit file is beyond the maximum number of files supported (two for AOS 6.7.1.R04, six for AOS 8.3.1.R01) then it is discarded.

The audit functionality can be also configured to send the audit events to an external syslog server using TLS for protecting the communication channel.

FAU_STG.1

The audit files are protected from deletion and modification. Only the Security Administrator can delete or modify the audit files.

7.1.2 Cryptographic Support

The TOE implements cryptographic protocols and algorithms using the following standard packages included in the TOE.

- For AOS 6.7.1.R04
  - OpenSSL v1.0.2g and OpenSSL FIPS Object Module SE v2.0.12 for TLSv1.1, TLSv1.2, and cryptographic algorithm support
  - OpenSSH v5.0 for implementing the SSHv2 protocol. OpenSSH uses OpenSSL for the underlying cryptographic algorithms
- For AOS 8.3.1.R01
  - OpenSSL v1.0.2j and OpenSSL FIPS Object Module SE v2.0.13 for TLSv1.1, TLSv1.2, and cryptographic algorithm support
  - OpenSSH v6.0p1 for implementing the SSHv2 protocol. OpenSSH uses OpenSSL for the underlying cryptographic algorithms

7.1.2.1 OpenSSL cryptographic module

OpenSSL implements versions 1.1 and 1.2 of the Transport Layer Security (TLS) protocol and cryptographic algorithms. The following table summarizes the cryptographic algorithms implemented in OpenSSL and used by the TOE to support communication protocols, protection of TSF data and authentication.

Cryptographic Services	Cryptographic Algorithms and Key Sizes	Usage / Purpose	AOS 6.7.1.R04	AOS 8.3.1.R01
Key Generation	RSA 2048-bit keys	● TLSv1.1 and TLSv1.2 ● SSHv2	✓	✓
	ECDSA P-256, P-384 and P-521 keys	● TLSv1.1 and TLSv1.2 ● SSHv2		✓
Key Establishment	RSA-based, 2048-bit keys	● TLSv1.1 and TLSv1.2 ● SSHv2	✓	✓
	ECDSA-based, P-256, P-384 and P-521 keys	● TLSv1.1 and TLSv1.2 ● SSHv2		✓

Cryptographic Services	Cryptographic Algorithms and Key Sizes	Usage / Purpose	AOS 6.7.1.R04	AOS 8.3.1.R01
Encryption / Decryption	AES in CBC mode, 128 and 256 bit keys	● TLSv1.1 and TLSv1.2 ● SSHv2	✓	✓
	AES in GCM mode, 128 and 256 bit keys	● TLSv1.1 and TLSv1.2		✓
Signature Generation and Verification	RSA with RSASSA-PSS and RSASSA-PKCS1v1_5 (SHA-1, SHA-256, SHA-384 and SHA-512)	● TLSv1.1 and TLSv1.2 ● SSHv2	✓	✓
	ECDSA with P-256, P-384, and P-521 keys, with SHA-256, SHA-384 and SHA-512	● TLSv1.1 and TLSv1.2 ● SSHv2		✓
Message Digest	SHA-1	● Signature Generation and Verification ● Keyed Hashing ● Password storage	✓	✓
	SHA-256	● Signature Generation and Verification ● Keyed Hashing ● Password storage	✓	✓
	SHA-384	● Keyed Hashing		✓
	SHA-512	● Keyed Hashing		✓
Keyed Hashing	HMAC-SHA-1	● TLSv1.1 and TLSv1.2 ● SSHv2	✓	✓
	HMAC-SHA1-96	● SSHv2	✓	✓
	HMAC-SHA-256	● TLSv1.1 and TLSv1.2 ● SSHv2	✓	✓
	HMAC-SHA-384	● TLSv1.1 and TLSv1.2		✓
	HMAC-SHA-512	● SSHv2		✓
DRBG	Hash_DRBG (default), CTR_DRBG, HMAC_DRBG	● Asymmetric key generation ● Session key generation	✓	✓

Table 14: Cryptographic Services and Algorithms

The following table provides additional information on the HMAC parameters supported by OpenSSL and used in the TOE:

Cryptographic Algorithm	Hash function	Block size (hash function)	Key Size	Output MAC length
HMAC-SHA-1	SHA-1	512 bits	256 bits	160 bits
HMAC-SHA-1-96	SHA-1	512 bits	256 bits	96 bits
HMAC-SHA-256	SHA-256	512 bits	256 bits	256 bits
HMAC-SHA-384	SHA-384	1024 bits	256 bits	384 bits
HMAC-SHA-512	SHA-512	1024 bits	256 bits	512 bits

Table 15: HMAC parameters

OpenSSL includes a Deterministic Random Bit Generator (DRBG) with a minimum of 256 bit of entropy. The DRBG uses the HASH_DRBG algorithm by default. If there is a failure in instantiation, the DRBG will fallback to CTR_DRBG as well as HMAC_DRBG.

OpenSSL performs the following power-up self-tests to ensure that the module and all validated cryptographic algorithms work properly:

- Integrity verification of the shared libraries that comprise the cryptographic module
- Known Answer Test (KAT) for symmetric encryption and decryption algorithms
- KAT for the DRBG
- KAT for MAC and message digest algorithms
- KAT for RSA signature generation and verification algorithms
- KAT for the ECC CDH algorithm
- Pair-wise Consistency Tests (PCT) for ECDSA asymmetric algorithms

OpenSSL also performs the following conditional tests during the execution of services.

- PCT on each generation of a RSA or ECDSA key pair

In case of failure of any of the power-up self-tests or conditional tests, OpenSSL raises an exception and the TOE shows an error message in the console, for instance:

"*Signature RSA test Failed Incorrectly!!*"

or

"*DRBG SHA256 test Failed Incorrectly!!*"

Once all self-tests are executed, and in case a failure was identified, OpenSSL shows a summary of the errors encountered and forces the TOE to restart. The following is the list of possible error messages:

"*FIPS routines:FIPS_check_incore_fingerprint:fingerprint does not match:fips.c:232:*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=SHA1 Digest*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=SHA1 Digest*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=SHA1 Digest*"

"*FIPS routines:FIPS_selftest_aes:selftest failed:fips_aes_selftest.c:98:*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=RSA SHA256 PSS*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=ECDSA P-224*"

"*FIPS routines:fips_pkey_signature_test:test failure:fips_post.c:340:Type=DSA SHA384*"

OpenSSL maintains in RAM all critical security parameters (CSP) used by the cryptographic services (DRBG internal state, session keys, etc.) requested by the TOE. OpenSSL clears with zeroes and deallocates all the memory used by the CSP when they are no longer needed.

7.1.2.2 Transport Layer Security (TLS) protocol

The TOE implements versions 1.1 and 1.2 of the TLS protocol provided by OpenSSL. The TOE establishes a secure channel using TLS for the following purposes:

- As a TLS client
  - Communication with an external audit server (syslog) for audit generation
  - Communication with an external LDAP server for using authentication credentials stored externally.
  - Communication with a RADIUS server for external authentication

The TOE allows single (server side) or mutual authentication (client and server side) through the use of X.509 certificates. The TOE performs certificate and certificate path validation of the server certificate during the TLS handshake. If the certificate cannot be successfully validated (e.g. it has expired or has been revoked) the TLS session is not established. See section 7.1.2.4 for more information.

For single authentication, it is the server end who presents the certificate during TLS handshake, so the TOE only parses the certificate from the TLS message and verifies that the server certificate is valid. For mutual authentication, though, the TOE also have to send the client certificate at the server's request. The TOE looks for the certificate and its private key at the certificate directory (/flash/switch for AOS 6.7.1.R04 or /flash/switch/cert.d for AOS 8.3.1.R01). The certificate and key must be named as **`myCliPrivate.key`** and **`myCliCert.pem`**, respectively.

The TOE also verifies that the certificate presented by the TLS server during the TLS handshake corresponds to the server. The TOE uses the DNS names included in the Subject Alternative Name (SAN) field as the reference identifier for the server certificate (there is no other reference identifier defined for this purpose and this feature cannot be configured by the administrator). If the server hostname matches one of the DNS names presented in the certificate, then the certificate is trusted. If there is no match or the server certificate does not include a DNS name, the TLS session is not established.

The TOE only allows the establishment of a TLS secure channel using TLSv1.1 or TLSv1.2. The TOE denies any attempt by a TLS client to establish communication using the following versions of the SSL or TLS protocols: SSLv1.0, SSLv2.0, SSLv3.0 or TLSv1.0.

The TOE creates session keys following the TLS protocol specification and using the DRBG implemented in OpenSSL. The TOE destroys session keys when the session is terminated by clearing with zeroes and deallocating the RAM memory used to store the session keys.

The following table enumerates the cipher suites supported by TLS in the two versions of the operating system supported by the TOE.

Cipher Suite	AOS 6.7.1.R04	AOS 8.3.1.R01
TLS_RSA_WITH_AES_128_CBC_SHA	✓	✓

Cipher Suite	AOS 6.7.1.R04	AOS 8.3.1.R01
TLS_RSA_WITH_AES_256_CBC_SHA	✓	✓
TLS_DHE_RSA_WITH_AES_128_CBC_SHA		✓
TLS_DHE_RSA_WITH_AES_256_CBC_SHA		✓
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		✓
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		✓
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		✓
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		✓
TLS_RSA_WITH_AES_128_CBC_SHA256	✓	✓
TLS_RSA_WITH_AES_256_CBC_SHA256	✓	✓
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		✓
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		✓
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		✓
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		✓
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256		✓
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384		✓
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256		✓
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384		✓

Table 16: TLS Cipher Suites supported by the TOE

The cipher suites are selected in the order shown in the table; there is no security management function to disable a cipher suite or alter the order in which they are chosen.

In AOS 8.3.1.R01 the TOE implements the Supported Elliptic Curves Extension according to [RFC4492] with NIST curves secp256r1, secp384r1, and secp521r1. The Supported Elliptic Curves Extension is performed following the order of cipher suites shown in the table above; there is no security management function to configure its behavior.

The following table shows the cryptographic keys involved in the TLS protocol, their location and how they are created and destroyed:

Key	Key Location	Purpose	Destruction
TLS server certificate (public key)	RAM (received from TLS server)	Server authentication Key establishment	Zeroization and deallocation when session is terminated

Key	Key Location	Purpose	Destruction
TLS client certificate (public and private keys)	`/flash/switch/myCliCert.pem` `/flash/switch/cert.d/myCliCert.pem`	Client authentication	Removal from filesytem through CLI commands
Session keys	RAM	Integrity and confidentiality during session	Zeroization and deallocation when session is terminated

Table 17: Keys used by the TLS protocol

7.1.2.3 Secure Shell version 2 (SSHv2) protocol

The TOE implements the Secure Shell version 2 (SSHv2) protocol using OpenSSH v5.0 (in AOS 6.7.1.R04) and v6.0p1 (in AOS 8.3.1.R01). Both packages use OpenSSL as the underlying layer for cryptographic algorithms.

The TOE establishes a secure channel using SSHv2 for the following purposes.

- As a SSHv2 server
    - Secure communication for SSHv2 clients used in Security Management (Command Line Interface)
    - Support for Secure File Transfer protocol (SFTP) clients
- As a SSHv2 client
    - Secure communication with remote SSH servers
    - SFTP client for remote SFTP servers

The SSHv2 protocol complies with [RFC4251]☝, [RFC4252]☝, [RFC4253]☝, [RFC4254]☝, [RFC5656]☝ and [RFC6668]☝. The following table shows the algorithms used for the different aspects of the SSHv2 protocol in the AOS supported by the TOE.

SSHv2 protocol aspect	Cryptographic Algorithm	AOS 6.7.1.R04	AOS 8.3.1.R01
Authentication Methods	Public Key based	✓	✓
	Password based	✓	✓
Encryption algorithms	AES (CBC mode) with 128-bit keys	✓	✓
	AES (CBC mode) with 256-bit keys	✓	✓
Public key algorithms	RSA with SHA-1	✓	✓
	ECDSA with SHA-2 and NIST curves P-256		✓
Data integrity MAC algorithms	HMAC-SHA1, HMAC-SHA1-96	✓	✓
	HMAC-SHA2-256	✓	✓
	HMAC-SHA2-512		✓

SSHv2 protocol aspect	Cryptographic Algorithm	AOS 6.7.1.R04	AOS 8.3.1.R01
Key Exchange methods	Diffie Hellman group 14 with SHA-1	✓	✓
	Elliptic Curve DIffie Hellman with SHA-2 and NIST curves P-256, P-384 and P-521		✓

Table 18: SSHv2 algorithms supported by the TOE

The TOE (acting as a SSHv2 server) supports SSHv2 sessions using SSH public key and password authentication by default. When a user attempts to establish a SSHv2 session, the TOE verifies that the user has a public key associated and the public key file exists on the switch (`/flash/switch/.profiles/.<username>_keys.pub`). If these conditions are met, then public key authentication is used, otherwise password authentication is used as the fallback authentication mechanism.

In addition, the TOE provides the **`ssh enforce pubkey-auth`** command in the CLI to enforce public key authentication only, thus disabling password based authentication. If public key authentication fails, then access to the switch is not granted.

When starting a SSHv2 session as a client in the TOE, the authentication mechanisms to be used in the session are enforced by the SSHv2 server. The TOE supports both SSH public key and password authentication. For SSH public key authentication, the `ssh`command issued by the administrator from the CLI must include the user's private key as a parameter and the key must exist in the flash filesystem.

The TOE limits the size of SSHv2 packets to 256 Kb; packets greater than this size in an SSH transport connection are dropped. In addition, the TOE also controls that the SSHv2 session does not transmit more than 2^28 packets with the same session key. If that threshold is surpassed, new session keys are established between both ends.

The TOE creates session keys following the SSHv2 protocol specification and using the DRBG implemented in OpenSSL. The TOE destroys session keys when the session is terminated by clearing with zeroes and deallocating the Random Access Memory (RAM) memory used to store the session keys.

SSHv2 public and private keys are created by the TOE administrator via the CLI. Keys are also deleted from the filesystem by the TOE administrator using filesystem commands from the CLI (e.g. rm). The TOE removes from the filesystem the file entry corresponding to the key .

The following table shows the cryptographic keys involved in the SSHv2 protocol, their location and how they are created and destroyed:

Key	Key Location	Purpose	Destruction
SSH host RSA public key	/flash/system/ssh_host_rsa_key.pub	Key Establishment	Removal from filesytem thgough CLI commands
SSH host RSA private key	/flash/system/ssh_host_rsa_key.pub	Key Establishment	
SSH host ECDSA public key	/flash/system/ssh_host_ecdsa_key.pub	Key Establishment	

Key	Key Location	Purpose	Destruction
SSH host ECDSA private key	/flash/system/ssh_host_ecdsa_key.pub	Key Establishment	
SSH user public key	/flash/system/<username>_rsa.pub	Public Key authentication	
SSH user private key	/flash/system/<username>_rsa	Public Key authentication	
Session keys	RAM	Integrity and confidentiality during session	Zeroization and deallocation when session terminates

Table 19: Keys used by the SSHv2 protocol

7.1.2.4 X.509 Certificate generation and validation

The TOE supports X.509 certificate validation and certificate path validation according to [RFC5280]. They are used during the TLS handshake procedure to verify trust on the certificate received from the TLS server, and verify the trust of the OCSP responder (if applicable).

For single authentication, the TLS server presents the certificate during the TLS handshake, so the TOE (acting as a TLS client) only parses the certificate from the TLS message and validates the server certificate. For mutual authentication, the TOE (acting as a TLS client) sends its certificate at the TLS server's request. The TOE certificate is located at the certificate directory (/flash/switch for AOS 6.7.1.R04 or /flash/switch/cert.d for AOS 8.3.1.R01) with the name **`myCliCert.pem`**.

Certificate validation and certificate path validation consist of the following steps:

1. Verify that the certificate has a correct format and has not expired.
2. Verify that the chain of trust from the certificate up to the CA root certificate is maintained.
3. Verify that the basicConstraints extension exists and the CA flag is set to TRUE for all CA certificates in the path.
4. Verify that the CA root certificate is trusted.
5. Verify that the certificate has not been revoked.
6. Verify that the extendedKeyUsage field in the certificate corresponds to the use of the certificate ("Client Authentication", "Server Authentication", "OCSP Signing" purpose).

If all these steps are successful, then the certificate is considered valid. If any of these steps fails, then the certificate is considered invalid.

The TOE obtains the revocation status of the certificate as follows:

- For AOS 6.7.1.R04, the TOE verifies if an OCSP URL is present in the certificate and validates its revocation status by sending a certificate status query to the OCSP responder. If the OCSP responder is not reachable (*Unknown* status) or if the OCSP URL is not present in the certificate, the TOE validates the certificate using the local CRL file (crl.pem) stored in the flash filesystem ("/flash/switch" directory). If the local CRL is not configured (e.g. the file is not present), then the validation fails and the certificate is assumed to be revoked.

- For AOS 8.3.1.R01, the TOE validates first the certificate using the local CRL file (crl.pem) stored in the flash filesystem ("/flash/switch/cert.d"). If the local CRL is not configured, then the OCSP responder is attempted. If the OCSP responser is not reachable (*Unknown* status) or if the OCSP URL is not present in the certificate, then the validation fails and the certificate is assumed to be revoked.

In either case, if the mechanism chosen for obtaining the certificate revocation status is available (i.e. the OCSP responds *OK* or *Revoked*, or the local CRL is properly configured), then the result is used to determine whether the certificate is revoked or not. As described above, whenever the mechanism is not available (the OCSP service does not responds or the CRL file does not exist), the TOE assumes the certificate status is revoked.

The TOE contains a default CA keystore located in the flash filesystem ("/flash/switch" directory in AOS 6.7.1.R04, "/flash/switch/ca.d" in AOS 8.3.1.R01). This keystore is used to perform certificate validation and contains all CA root certificates that are trusted by the TOE. The same directory contains the CRL used for local validation of the certificate revocation.

The TOE supports generation of RSA-based certificates. The TOE includes commands in the CLI to generate a Certificate Signing Request (CSR) and receive the corresponding CA certificate response file. After the CSR file is generated by the TOE, the administrator sends the request to a CA for being signed. Once the CA certificate response is received, the administrator uses the CLI to validate the certificate chain and import the signed certificate into the TOE.

RSA-based as well as ECDSA-based certificates can be generated outside the TOE and imported and configured in the TOE using the CLI.

The TOE provides the **`certificate delete`** command in the CLI to remove certificates and their associated keys from the filesystem.

7.1.2.5 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FCS_CKM.1 / AOS6.7.1

The TOE generates RSA asymmetric cryptographic keys that are used to protect communications for TLSv1.1, TLSv1.2 and SSHv2.

FCS_CKM.1 / AOS8.3.1

The TOE generates RSA and ECDSA asymmetric cryptographic keys that are used to protect communications for TLSv1.1, TLSv1.2 and SSHv2.

FCS_CKM.2 / AOS6.7.1

The TOE performs key establishment based on RSA asymmetric cryptographic keys that are used to protect communications for TLSv1.1, TLSv1.2 and SSHv2.

FCS_CKM.2 / AOS8.3.1

The TOE performs key establishment based on RSA and ECDSA asymmetric cryptographic keys that are used to protect communications for TLSv1.1, TLSv1.2 and SSHv2.

FCS_CKM.4

The TOE destroys key material by overwriting it with zeroes and releasing the allocated memory only after a read-verify to ensure it was properly zeroized.

FCS_COP.1(1) / AOS6.7.1

OpenSSL implements AES encryption and decryption in accordance to these SFRs.

FCS_COP.1(1) / AOS8.3.1

OpenSSL and the kernel crypto library in AOS 8.3.1.R01 implement AES encryption and decryption in accordance to these SFRs.

FCS_COP.1(2) / AOS6.7.1

OpenSSL implements RSA signature generation and verification in accordance to these SFRs.

FCS_COP.1(2) / AOS8.3.1

OpenSSL implements RSA and ECDSA signature generation and verification in accordance to these SFRs.

FCS_COP.1(3) / AOS6.7.1

OpenSSL implements SHA-1 and SHA-2 hashing algorithms in accordance to these SFRs.

FCS_COP.1(3) / AOS8.3.1

OpenSSL implements SHA-1 and SHA-2 hashing algorithms in accordance to these SFRs.

FCS_COP.1(4) / AOS6.7.1

OpenSSL implements HMAC-SHA-1 and HMAC-SHA-2 keyed hashing algorithms in accordance to these SFRs.

FCS_COP.1(4) / AOS8.3.1

OpenSSL and the kernel crypto library in AOS 8.3.1.R01 implement HMAC-SHA-1 and HMAC-SHA-2 keyed hashing algorithms in accordance to these SFRs.

FCS_RBG_EXT.1

OpenSSL implements DRBG algorithms in accordance to this SFR. The TOE provides an entropy source for seeding the DRBG with a minimum of 256 bits.

FCS_SSHC_EXT.1 / AOS6.7.1, FCS_SSHC_EXT.1 / AOS8.3.1

OpenSSH implements the SSHv2 protocol in accordance to these SFRs.

FCS_SSHS_EXT.1 / AOS6.7.1, FCS_SSHS_EXT.1 / AOS8.3.1

OpenSSH implements the SSHv2 protocol in accordance to these SFRs.

FCS_TLSC_EXT.2 / AOS6.7.1, FCS_TLSC_EXT.2 / AOS8.3.1

OpenSSL implements the TLSv1.1 and TLSv1.2 protocols in accordance to these SFRs. The TOE supports the cipher suites selected in these SFRs.

FIA_X509_EXT.1

The TOE performs X.509 certificate validation using the Online Certificate Status Protocol (OCSP), as specified in [RFC2560]☝, and using a Certificate Revocation List (CRL), as specified in [RFC5759]☝.

FIA_X509_EXT.2

The TOE supports X.509 certificate validation for the TLSv1.1 and TLSv1.2 protocols.

FIA_X509_EXT.3

The TOE supports the generation of Certificate Request Messages as specified by [RFC2986]☝ and processing of the CA Certificate Response.

7.1.3 Identification and Authentication of TOE Administrators

The TOE provides local and remote access to administrators; local access is provided through the serial console (connected to the available ports), whereas remote access is provided through the SSHv2 protocol using an SSHv2 client. A local or remote session can be terminated by the administrator at any time.

Before a local or remote session is established, a banner is displayed to the user that attempts to log into the TOE. An administrator of the TOE can modify the content of this banner to display warnings or advisory notices that reflect the security policy of the organization.

The TOE requires the administrator to identify and authenticate to the TOE prior to accessing any of the management functionality regardless of the mechanism being used to interface with the TOE (via the serial console, SSH, SFTP).

There is one default user account provided with the TOE: *admin*. The *admin* user account is the initial administrator assigned all privileges. The *admin* user account is used to install and setup the TOE.

The TOE also provides a default user configuration used to store user defaults for assigning privileges and profile information to newly created users. The default user configuration cannot be used to log into the switch.

Authentication can be performed locally on the TOE or the TOE can send a request to an external authentication server in the operational environment to verify the identity of the user. The method of authentication required by the TOE is configured based on the interface used to access the TOE. The only external authentication server supported by the TOE for administrator authentication is RADIUS (TACACS+ is not allowed in the evaluated configuration). The TOE can also use an external LDAP server for storing authentication credentials. In both cases, the LDAP and RADIUS servers are part of the operational environment.

When configured for local authentication, the TOE maintains administrative-user security attributes of identifier (user ID), password information (authentication data), and user privileges (authorizations or user profile) and roles. The authentication data (password) is hashed prior to being stored using SHA-1 (in AOS 6.7.1.R04) or SHA-256 (in AOS 8.3.1.R01). These attributes are stored locally on the flash file system, in directories protected from read and write access from the administration console.

If the user and password information match the authentication data stored in the TOE, authentication succeeds and the user is granted access.

When an external authentication server is used, the external authentication server is responsible for storing, maintaining, and communicating the user's security attributes. The TOE sends the user and password information provided by the administrator; the external authentication server then verifies the credentials and returns the result of the identification and authentication operation.

The TOE provides the following user authentication failure settings:

- *Lockout window*: The length of time a failed user login attempt is aged before it is no longer counted as a failed user login attempt. The valid range is 0 to 99,999. The number of failed login attempts is decremented by the number of failed attempts that age beyond the lockout window. The default lockout window is set to 0, which means that all consecutive failed login attempts are counted, regardless of how much time has elapsed between the failed logins.

- *Lockout threshold*: The number of failed user login attempts allowed within a given lockout window period of time (0-999). The default lockout threshold is set to 0, which means that there is no limit to the number of failed login attempts allowed.
- *Lockout duration*: The length of time a user account remains locked out until it is automatically unlocked. The valid range is 0 to 99,999. The default lockout duration is set to 0, which means that there is no automatic unlocking of a user account by the switch.

When authentication is performed locally by the TOE, the TOE ensures that if the number of failed user login attempts exceeds the lockout threshold during the lockout window period of time, the user account is locked out of the switch for the lockout duration (this behavior does not apply to the default *admin* account). The user’s authentication failure counter is reset when the user successfully authenticates.

When an external authentication server is used, the external authentication server is responsible for locking out the user.

The TOE monitors the time of inactivity of local and remote sessions, forcing the termination of a session when the timeout interval has been reached.

- The login attempt session timeout defines the amount of time the administrator can take to accomplish a successful login to the switch. If the login timeout period is exceeded, the TCP connection is closed by the switch. The default login timeout period is 55 seconds.
- The user session timeouts define the amount of time the user can be inactive for CLI and SFTP sessions. When the TOE detects no user activity for the administrator configured period of time, the user is logged off the TOE. The default timeout for CLI and SFTP sessions is four minutes.

The TOE provides global password settings used to implement and enforce local password complexity when a password is created or modified. The password settings available on the TOE are:

- *Minimum Password Length*: The number of characters required when configuring a user password. The default value is 15 characters and can be changed within the range of 15 to 30 characters.
- *Password Expiration*: The number of days before user passwords will expire. The allowed range is 1-150 days. Password expiration is disabled by default.
- *Username not allowed*: Specifies whether or not the password is allowed to contain the username. The default is to allow the password to contain the username.
- *Minimum Uppercase characters*: Specifies the minimum number of uppercase characters required for a user password. The allowed range is 0-7. By default, there is no required minimum number of uppercase characters.
- *Minimum Lowercase characters*: Specifies the minimum number of lowercase characters required for a user password. The allowed range is 0-7. By default, there is no required minimum number of lowercase characters.
- *Minimum Numeric characters*: Specifies the minimum number of numeric characters (base-10 digits) required for a user password. The allowed range is 0-7. By default, there is no required minimum number of numeric characters.
- *Minimum non-alpha characters*: Specifies the minimum number of non-alphanumeric characters (symbols) required for a user password. The allowed range is 0-7. By default, there is no required minimum number of non-alpha characters.
- *Password History*: Specifies the maximum number of old passwords to retain. The range is 0-24 and the default is to retain 4 old passwords. The user is prevented from reusing any retained passwords. A value of 0 disables the password history function.

- *Minimum Password Age*: Specifies the minimum number of days during which the user is prevented from changing a password. The allowed range is 0-150. By default, there is no required minimum number of days.

When authentication is performed through a local session, the TOE does not display the password characters; instead, an asterisk is echoed for each character input.

7.1.3.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FIA_PMG_EXT.1
The TOE allows the configuration of a password policy that includes a minimum length, and the combination of upper and lower case, numbers and special characters.

FIA_UIA_EXT.1
The TOE displays a warning banner before an administrative user attempts to login through a local (serial) or remote (SSHv2 client) console.

FIA_UAU_EXT.2, FIA_UAU.7
The TOE provides a password-based authentication mechanism, where passwords are not shown during the identification and authentication process.

FTA_SSL_EXT.1
The TOE terminates local sessions after a period of inactivity.

FTA_SSL.3
The TOE terminates remote sessions after a period of inactivity.

FTA_SSL.4
An Administrator can terminate a local or remote session at any time.

FTA_TAB.1
The TOE allows the configuration of a banner shown to the user before an interactive session is established.

7.1.4 Security Management

The TOE provides the following management functions for use by security administrators.

- Set the date and time
- Enable, disable or configure use of remote authentication servers (RADIUS, LDAP)
- Configure Ethernet Ports
- Terminate another administrator session
- Enable, disable and configure audit parameters
- Configure user login attempt lockout settings
- Configure failed session login attempt settings
- Configure password policy settings
- Configure session timeout intervals

Security management function can be performed through a CLI. The CLI can be accessed from the serial console or through a SSHv2 client. In addition, the Flash file system on the switch provides the ability to store and edit configuration files that can be transferred to and from the Flash file system via SFTP. SNMP is also supported as a security management interface but it is not allowed in the evaluated configuration.

Acting on behalf of a security administrator, the CLI requests security management operations from the same underlying service in the TOE. Therefore, although there are different methods of use for requesting the security management functions, each method utilizes the same underlying software to actually perform the functions.

Use of each of these management functions is restricted to the authorized administrator by requiring the administrator to successfully identify and authenticate to the TOE prior to allowing access to the functions. In addition, administrators are assigned read-only or read-write access to the command families available on the switch. The command families correspond to the commands categories available via the three interfaces. Examples of command families include file, system, config, module, interface, ip, vlan, dns, qos, policy, session, aaa.

There is a single role of Administrator for the TOE. Administrators are granted access to management functions based on the access granted to their user account. The TOE provides the ability to grant read-only or read-write access to the command families available on the switch. The command families correspond to the commands categories available via the three interfaces. Examples of command families include file, system, config, module, interface, ip, vlan, dns, qos, policy, session, aaa. The aaa command family provides the ability to configure the type of authentication methods supported by the switch and perform user account management.

7.1.4.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FMT_MOF.1(1) / Audit, FMT_MOF.1(2) / Audit, FMT_MOF.1(1) / AdminAct
The TOE restricts security administrators to determine and modify the behavior of security functions.

FMT_MOF.1(1) / TrustedUpdate
The TOE restricts security administrators to perform manual updates of the TOE software.

FMT_MTD.1
The TOE restricts security administrators to manage TSF data.

FMT_MTD.1 / AdminAct
The TOE restricts security administrators to manage cryptographic keys.

FMT_SMF.1
The TOE provides the security management functions specified in this SFR.

FMT_SMR.2
The TOE supports the Security Administrator role, who is the only role authorized to access the TOE locally and remotely.

7.1.5 Protection of the TSF

Passwords are stored in non-plaintext form using a hashing algorithm: SHA-256 in AOS 8.3.1.R01, and SHA-1 in AOS 6.7.1.R04. The hashed value of the password is stored in a directory of the flash filesystem protected from read and write access.

The TOE uses the service of external IT entities to support different aspects of the security functionality. The TOE ensures that communications between the TOE itself and these external IT entities are protected using a trusted communication channel.

The TOE also provides a trusted communication path using the SSHv2 protocol for sessions remotely initiated by administrators.

The following table describes the services used by the TOE and how they are protected.

Purpose	External IT entity	Secure channel
Audit record generation	Syslog server	TLSv1.1 or TLSv1.2
External authentication	RADIUS server	TLSv1.1 or TLSv1.2
External storage for credentials	LDAP server	TLSv1.1 or TLSv1.2
SSH requests	SSH client/server	SSHv2
SFTP requests	SFTP client/server	SSHv2

Table 20: Trusted channels

The TOE includes the OpenSSL cryptographic module, which supports the TLS protocol and the underlying cryptographic algorithms used by the TOE. The cryptographic module performs power-on self-tests (POST) to ensure the integrity of the module itself and the correct behavior of the cryptographic algorithms, and conditional tests to ensure that asymmetric pair keys are correctly generated. Please refer to section 7.1.2.1 for a detailed description of the tests performed by the module.

The POST proceeds until all self-tests are completed, and the TOE writes an audit record for each self-test that failed. In case of a failure in any of the self-tests, the TOE is forced to reload and reinitialize the operating system, thus performing the POST again. This mechanism ensures that no cryptographic algorithm is available until all self-tests are successful. Please refer to section 7.1.2.1 for a detailed description of the self-test error messages that the module may show.

The TOE prevents access to all pre-shared keys, symmetric keys and private keys from the CLI by using operating system's file access control: access to directories containing files with sensitive material is denied for all configured administrative users. The admin user, which is the default user in the TOE, is the only user that can have access to the files but its use is restricted to the installation and the initial configuration of the TOE.

The TOE does not provide a mechanism for automatic updates of the TOE; instead, the TOE provides via the CLI several commands for installing and updating the TOE in a secure way:

- Download the new version of the TOE and the corresponding SHA-256 hash value (firmware image and hash value files) from the vendor using a secure transfer method (`sftp`).
- Visualize the currently active version of the TOE, and the most recently installed version of the TOE (`show microcode` command).
- Verify the integrity of the downloaded image file that represents the TOE firmware against the SHA-256 hash value (`image integrity-check`.
- Reload the TOE using the new version of the TOE firmware, verifying its integrity against the SHA-256 hash value (`reload from`).

If the integrity of the TOE image is verified successfully, the command can proceed and the new version of the TOE is installed. If the integrity verification fails, then the TOE image is rejected and the command does not proceed with the update. The administrator is responsible of following the instructions included in the TOE guidance to securely download, and install and/or update the TOE.

The TOE does not provide a means for installing a trusted update of the TOE with a delayed activation. However, the administrator must reboot the TOE in order to make the changes effective.

The TOE provides a reliable date and time for the following security functions:

- Generation of a timestamp for audit events.
- Verification of the expiration of the certificate in X.509 certificate validation.
- Calculation of period of inactivity of an interactive session to evaluate the termination of local and remote sessions.

The TOE obtains the date and time from an internal system clock. This system clock can be updated by the security administrator through the CLI.

7.1.5.1 SFR coverage

The TOE security functionality satisfies the following security functional requirements.

FPT_SKP_EXT.1
The TOE stores key material in directories of the flash filesystem which are protected from read/access from any user, including administrators.

FPT_APW_EXT.1
The TOE stores the hashed value of the password in a directory of the flash filesystem that is protected from read/access from any user, including administrators.

FPT_TST_EXT.1
The TOE uses OpenSSL which is a FIPS 140-2 validated cryptographic module. The module performs self-tests during start-up and conditional tests, which ensures the correct operation of the cryptographic algorithms.

FPT_TUD_EXT.1
The TOE allows administrators to verify the executing version and the most recently installed version of the TOE software. It also allows manual updates of the TOE software, verifying its trust and integrity using a published hash before being installed.

FPT_STM.1
The TOE has an internal system clock which is used to generate reliable timestamps.

FTP_ITC.1
All communications between the TOE and external IT entities are protected using a secure channel via TLSv1.1, TLSv1.2 or SSHv2 protocols.

FTP_TRP.1
All communications initiated by remote administrators to the TOE are protected using a secure channel via the SSHv2 protocol.

8 Abbreviations, Terminology and References

8.1 Abbreviations

AC
Alternating Current

ACL
Access control List

AES
Advanced Encryption System

AH
Authentication Header

ALE
Alcatel-Lucent Enterprise

AOS
Alcatel-Lucent Operating System

ARM
Advanced RISC Machine

ASA
Authenticated Switch Access

ASIC
Application-Specific Integrated Circuit

BGP
Border Gateway Protocol

BOOTP
Bootstrap Protocol

CBC
Cipher Block Chaining

CLI
Command Line Interface

CMM
Chassis Management Module. Physically a separate blade for 9000 series switches. Logically a separate piece of functionality built into the Management of the 6850E series

CN
Common Name

CRL
Certificate Revocation List

CSP
Critical Security Parameter

CSR
Certificate Signing Request

DC
Direct Current

DCB
Data Center Bridging

DHCP
Dynamic Host Configuration Protocol

DNS
Domain Name Server

DRBG
Deterministic Random Bit Generator

DSA
Digital Signature Algorithm

DVMRP
Distance Vector Multicast Routing Protocol

EAP
Extensible Authentication Protocol

ECD
Extended Component Definition

ECDH
Elliptic Curve Diffie-Hellman

ECDHE
Elliptic Curve Diffie-Hellman Exchange

ECDSA
Elliptic Curve Digital Signature Algorithm

ESP
Encapsulating Security Payload

GigE
Gigabit Ethernet

GNI
Gigabit Ethernet Network Interface

HDMI
High-Definition Multimedia Interface

HMAC
Keyed-Hash Message Authentication Code

HPoE
High Power over Ethernet

HTTPS
Hypertext Transfer Protocol Secure

IGMP
Internet Group Management Protocol

IKE
Internet Key Exchange

IP
Internet Protocol

IPv4
Internet Protocol version 4

IPv6
Internet Protocol version 6

IPX
Internetwork Packet Exchange

KAT
Known Answer Test

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

NI
Network Interface Module

NTP
Network Time Protocol

OCSP
Online Certificate Status Protocol

OS10K
Alcatel-Lucent Enterprise OmniSwitch 10K Series with AOS 8.3.1.R01

OS6250
Alcatel-Lucent Enterprise OmniSwitch 6250 Series with AOS 6.7.1.R04

OS6350
Alcatel-Lucent Enterprise OmniSwitch 6450 Series with AOS 6.7.1.R04

OS6450
Alcatel-Lucent Enterprise OmniSwitch 6350 Series with AOS 6.7.1.R04

OS6860
Alcatel-Lucent Enterprise OmniSwitch 6860 Series with AOS 8.3.1.R01

OS6865
Alcatel-Lucent Enterprise OmniSwitch 6865 Series with AOS 8.3.1.R01

OS6900
Alcatel-Lucent Enterprise OmniSwitch 6900 Series with AOS 8.3.1.R01

OS9900
Alcatel-Lucent Enterprise OmniSwitch 9900 Series with AOS 8.3.1.R01

OSPF
Open Shortest Path First

PAE
Port Access Entity

PCB
Printer Circuit Board

PCT
Pair-wise Consistency Test

PIM
Protocol-Independent Multicast

PoE
Power over Ethernet

PoH
Power over HD Base-T

PTP
Precision Time Protocol

QNI
40-Gigabit Ethernet Network Interface

QoS
Quality of Service

QSFP
Quad Small Form-factor Pluggable

RADIUS
Remote Authentication Dial In User Service

RIP
Routing Information Protocol

RSA
Rivest Shamir Adleman (cryptosystem)

SAN
Subject Alternative Name

SFP
Small Form-factor Pluggable transceiver (used in section 1.5.2.1.1) or Security Function Policies (used in the rest of the ST)

SFTP
Secure File Transfer Protocol

SLB
Server Load Balancing

SNMP
Simple Network Management Protocol

SPB
Shortest Path Bridging

SPD
Security Policy Database

SPI
Security Parameter Index

SSH
Secure Shell

SSHv2
Secure Shell version 2

STP
Spanning Tree Algorithm and Protocol

TACACS+
Terminal Access Controller Access-Control System Plus

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security

UDP
User Datagram Protocol

UNP
Universal Network Profile

USB
Universal Serial BUS

VIP
Virtual IP

VLAN
Virtual LAN

VoIP
Voice Over IP

VXLAN
Virtual Extensible Local Area Network

XNI
10-Gigabit Ethernet Network Interface

8.2 Terminology

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

Administrative-user
An administrative user of the TOE, authorized to control TOE settings, as opposed to end-users, associated with general network traffic

Appletalk
AppleTalk protocol. Also captures Datagram Delivery Protocol (DDP) and AppleTalk ARP (AARP)

Application
In the context of AOS auditing there are several ‘applications’ that log records. These are identified by a number and abbreviation.

Authenticated VLANs
Authenticated VLANs control operator access to network resources based on VLAN assignment and a operator log-in process

Decnet
DECNET Phase IV (6003) protocol

End-user
Network traffic, non-administrative users of the TOE

Fixed-configuration Switch
A network switch where the number of ports cannot be changed, when compared to a chassis type product.

IEEE 802.1X
IEEE 802.1X is an IEEE Standard for port-based Network Access Control

MAC Address
Media Access Control Address, also known as the hardware or adaptor address.

Port Mobility
The ability for the Alcatel-Lucent Switches to dynamically tag incoming traffic into a specific VLAN irrespective of the physical port the traffic enters

Power over Ethernet
Power over Ethernet (PoE) provides inline power directly from the switch’s Ethernet ports. Powered Devices (PDs) such as IP phones and wireless APs can be powered directly from the switch’s RJ-45 ports.

Stackable Switch
Network switch that can be connected with a special function cable with other stackable switches to function as a virtual chassis using a central management point

UNP
A Universal Network Profile comprises a set of policies that can be dynamically assigned to physical devices or end-users via authentication or by matching predefined criteria.

VLAN, (Virtual LAN) / Logical Network
The term VLAN was specified by IEEE 802.1Q; it defines a method of differentiating traffic on a LAN by tagging the Ethernet frames. By extension, VLAN is used to mean the traffic separated by Ethernet frame tagging or similar mechanisms. In this ST Logical network and VLAN are used interchangeably

WebView
The web based GUI to manage the TOE

8.3 References

AOS6-CCGUIDE **Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS Release 6.7.1.R04**
Version Part No. 060422-10 Rev. C
Date February 2017

AOS6-CLI **OmniSwitch AOS Release 6250/6350/6450 CLI Reference Guide**
Version Part No. 060440-10 Rev. A
Date October 2016

AOS6-NC **OmniSwitch AOS Release 6250/6350/6450 Network Configuration Guide**
Version Part No. 040439-10 Rev. A
Date October 2016

AOS6-RN **Release Notes - OmniSwitch 6250 / 6350 / 6450**
Version Part No. 033168-10 Rev. A
Date February 2017

AOS6-SM **OmniSwitch AOS Release 6250/6350/6450 Switch Management Guide**
Version Part No. 060438-10 Rev. A
Date October 2016

AOS6-TCV **OmniSwitch 6250/6350/6450 Transceivers Guide**
Version Part No. 060441-10 Rev. A
Date October 2016

AOS8-ARC **OmniSwitch AOS Release 8 Advanced Routing Configuration Guide**
Version Part No. 060413-10 Rev. A
Date September 2016

AOS8-CCGUIDE **Preparation and Operation of Common Criteria Evaluated OmniSwitch Products - AOS Release 8.3.1.R01**
Version Part No. 060417-00 Rev. C
Date February 2017

AOS8-CLI **OmniSwitch AOS Release 8 CLI Reference Guide**
Version Part No. 060415-10 Rev. B
Date February 2017

AOS8-DCS **OmniSwitch AOS Release 8 Data Center Switching Guide**
Version Part No. 060414-10 Rev. A
Date September 2016

AOS8-NC **OmniSwitch AOS Release 8 Network Configuration Guide**
Version Part No. 060412-10 Rev. A
Date September 2016

AOS8-RN **Release Notes - OmniSwitch 10K/9900/6900/6860(E)/6865**
Version Part No. 033169-10 Rev. A
Date February 2017

AOS8-SM **OmniSwitch AOS Release 8 Switch Management Guide**
Version Part No. 060411-10 Rev. A
Date September 2016

AOS8-TCV **OmniSwitch AOS Release 8 Transceivers Guide**
Version Part No. 060416-10 Rev. A
Date September 2016

CC **Common Criteria for Information Technology Security Evaluation**
Version 3.1R4
Date September 2012
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf

ND-cPPv1.0 **Collaborative Protection Profile for Network Devices Version 1.0**
Version 1.0
Date 2015-02-27
Location https://www.niap-ccevs.org/pp/cpp_nd_v1.0.pdf

OS10K-GS **OmniSwitch 10K Getting Started Guide**
Version Part No. 060309-10 Rev. A
Date September 2016

OS10K-HWUG **OmniSwitch 10K Hardware Users Guide**
Version Part No. 060310-10, Rev. J
Date September 2016

OS6250-HWUG **OmniSwitch 6250 Hardware Users Guide**
Version Part No. 060303-10, Rev. G
Date October 2016

OS6350-HWUG **OmniSwitch 6350 Hardware Users Guide**
Version Part No. 060406-10, Rev. D
Date February 2017

OS6450-HWUG **OmniSwitch 6450 Hardware Users Guide**
Version Part No. 060351-10, Rev. K
Date October 2016

OS6860-HWUG **OmniSwitch 6860/6860E Hardware Users Guide**
Version Part No. 060390-10, Rev. D
Date September 2016

OS6865-HWUG **OmniSwitch 6865 Hardware Users Guide**
Version Part No. 060435-10, Rev C
Date January 2017

OS6900-HWUG **OmniSwitch 6900 Hardware Users Guide**
Version Part No. 060334-10, Rev. L
Date September 2016

OS9900-HWUG **OmniSwitch 9900 Series Hardware Users Guide**
Version Part No. 060409-10, Rev C
Date February 2017

RFC2560 **X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP**
Author(s) M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams
Date 1999-06-01
Location http://www.ietf.org/rfc/rfc2560.txt

RFC2986 **PKCS #10: Certification Request Syntax Specification Version 1.7**
Author(s) M. Nystrom, B. Kaliski
Date 2000-11-01
Location http://www.ietf.org/rfc/rfc2986.txt

RFC3268 **Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)**
Author(s) P. Chown
Date 2002-06-01
Location http://www.ietf.org/rfc/rfc3268.txt

RFC4251 **The Secure Shell (SSH) Protocol Architecture**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4251.txt

RFC4252 **The Secure Shell (SSH) Authentication Protocol**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4252.txt

RFC4253 **The Secure Shell (SSH) Transport Layer Protocol**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4253.txt

RFC4254 **The Secure Shell (SSH) Connection Protocol**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4254.txt

RFC4346 **The Transport Layer Security (TLS) Protocol Version 1.1**
Author(s) T. Dierks, E. Rescorla
Date 2006-04-01
Location http://www.ietf.org/rfc/rfc4346.txt

RFC4492 **Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)**
Author(s) S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, B. Moeller
Date 2006-05-01
Location http://www.ietf.org/rfc/rfc4492.txt

RFC5246 **The Transport Layer Security (TLS) Protocol Version 1.2**
Author(s) T. Dierks, E. Rescorla
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5246.txt

RFC5280 **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**
Author(s) D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk
Date 2008-05-01
Location http://www.ietf.org/rfc/rfc5280.txt

RFC5289 **TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)**
Author(s) E. Rescorla
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5289.txt

RFC5656 **Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer**
Author(s) D. Stebila, J. Green
Date 2009-12-01
Location http://www.ietf.org/rfc/rfc5656.txt

RFC5759 **Suite B Certificate and Certificate Revocation List (CRL) Profile**
Author(s) J. Solinas, L. Zieglar
Date 2010-01-01
Location http://www.ietf.org/rfc/rfc5759.txt

RFC6125 **Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)**
Author(s) P. Saint-Andre, J. Hodges
Date 2011-03-01
Location http://www.ietf.org/rfc/rfc6125.txt

RFC6668 **SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol**
Author(s) D. Bider, M. Baushke
Date 2012-07-01
Location http://www.ietf.org/rfc/rfc6668.txt