Gigamon GigaVUE

Security Target

ST Version: 1.0
August 21, 2018

Gigamon, Inc.
3300 Olcott Street
Santa Clara, CA 95054

Prepared By:

Booz | Allen | Hamilton

delivering results that endure

Cyber Assurance Testing Laboratory
1100 West St
Laurel, MD 20707

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation.

1.1.1 ST Identification

ST Title: Gigamon GigaVUE Security Target
ST Version: 1.0
ST Publication Date: August 21, 2018
ST Author: Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this document provides identifying information for the ST and TOE as well as a brief description of the TOE and its associated TOE type.

Chapter 2 describes the TOE in terms of its physical boundary, logical boundary, exclusions, and dependent Operational Environment components.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the threats, assumptions, objectives, and organizational security policies that apply to the TOE.

Chapter 5 defines extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 6 describes the SFRs that are to be implemented by the TSF.

Chapter 7 describes the SARs that will be used to evaluate the TOE.

Chapter 8 provides the TOE Summary Specification, which describes how the SFRs that are defined for the TOE are implemented by the TSF.

1.1.3 Terminology

This section defines the terminology used throughout this ST. The terminology used throughout this ST is defined in Table 1 and 2. These tables are to be used by the reader as a quick reference guide for terminology definitions.

Term	Definition
Administrator	A user who is assigned the Admin role on the TOE and has the ability to manage the TSF.

Table 1-1: Customer Specific Terminology

Term	Definition
Security Administrator	The claimed Protection Profile defines a single Security Administrator role that is authorized to manage the TOE and its data. This TOE defines three separate user roles, but only the most privileged role (Admin) is authorized to manage the TOE's security functionality and is therefore considered to be the Security Administrator for the TOE.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application a Security Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to access the TOE functions or data.

Table 1-2: CC Specific Terminology

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 3. This table is to be used by the reader as a quick reference guide for acronym definitions.

Acronym	Definition
CC	Common Criteria
CLI	Command-Line Interface
cPP	collaborative Protection Profile
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RBG	Random Bit Generator
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

Table 1-3: Acronym Definition

1.1.5 References

[1] collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314 [NDcPP]

[2] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003

[5] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004

[6] ISO/IEC 18033-3:2010, Information Technology-Security techniques-Encryption algorithms—Part3: Block ciphers

[7] ISO/IEC 10116:2017, Information Technology-Security techniques-Modes of operation for an n-bit block cipher

[8] ISO/IEC 9796-2:2010, Information Technology -- Security techniques -- Digital signature schemes giving message recovery—Part 2 Integer factorization based mechanisms

[9] ISO/IEC 14888-3:2016, Information Technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms

[10] ISO/IEC 10118-3:2004, Information Technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions

[11] ISO/IEC 9797-2:2011, Information Technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function

[12] ISO/IEC 18031:2011, Information Technology -- Security techniques -- Random bit generation

[13] NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009

[14] FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[15] FIPS PUB 180-3, Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008

[16] FIPS PUB 180-4, Federal Information Processing Standards Publication Secure Hash Standard (SHS) August 2015

[17] NIST Special Publication SP800-56A Revision 2: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013

[18] NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators June 2015

[19] FIPS PUB 198-1, Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008

1.2 TOE Reference

The TOE is the Gigamon GigaVUE family of products, which includes the following appliance models:

GigaVUE-HD8, GigaVUE-HD4, GigaVUE-HC3, GigaVUE-HC2, GigaVUE-HC1, GigaVUE-TA100, GigaVUE-TA40, GigaVUE-TA10.

Each appliance runs the Gigamon GigaVUE-OS software version 5.1.01.

1.3 TOE Overview

The Gigamon GigaVUE Visibility Appliance (also known as GigaVUE or the TOE) is a network device that includes hardware and software. In the evaluated configuration, the TOE is a standalone device that is not deployed as a distributed TOE. The GigaVUE is a family of products that provide different performance and capability specifications; the TOE includes the models listed in section 1.2 above. These devices can be accessed locally via serial port and remotely via SSH CLI and TLS/HTTPS web GUI.

The GigaVUE's primary functionality is to use the Gigamon Forwarding Policy to receive out-of-band copied network data from external sources (TAP or SPAN port) and forward that copied network data to one or many tool ports for packet capture or analyzing tools based on user selected criteria. GigaVUE can also copy the network traffic itself when sitting in-line with the network flow using passive, inline and bypass taps or any combination. GigaVUE features extensive filtering abilities enabling authorized users to forward precise customized data flows of copied data from many sources to a single tool, from a single source to many tools, or from many sources to many tools.

A GigaVUE model:

- Receives a copy (or copies internally) network traffic
- Filters copied data based upon user selected criteria
- Forwards copied data to user selected ports

GigaVUE receives data from many sources, or networks. It can receive data from a 3rd party TAP or SPAN port. The GigaVUE can also be configured to be its own TAP. The internal TAP can be electrical so that it sits in line and copies the data, allowing the network traffic to continue to flow through unimpeded. GigaVUE also features an optical TAP that sits in line with production network and splits the light passing through the optical splitter making a copy of the network traffic.

GigaVUE can also act as a bypass TAP or a GigaTap. In this configuration, GigaVUE connects to both sides of an IPS or other in-line device and monitors both itself and the in-line device. Specifically, the GigaVUE copies network traffic creating copied network data, filters it, and sends it to tools. The GigaVUE Bypass TAP will then forward the data to the IPS or other in-line device, allow the device to perform its own designated functionality, and then receive the data again from the same device. The GigaVUE will then process the data a second time using the same functionality to copy the network traffic after the in-line device process. Then the GigaVUE Bypass TAP will send the network traffic out to the production network. The GigaTap is a TAP that has the ability to split and copy inbound or outbound data streams.

GigaVUE forwards the data received via a network port to a tool port based on user configured policy. Tool ports are physically connected to a packet capture or other analyzing tools. Any type of tool can be attached to the tool port such as an IDS, forensic data recorder, sniffer, or protocol analyzer.

Multiple GigaVUE devices can also be physically connected over a stacking port in order to perform load balancing or to use a larger number of tools than is supported by a single device. However, this distributed model is outside the scope of the evaluated configuration. The TOE was evaluated as a standalone network device only and the GigaVUE's network traffic capture, filter, and forwarding

capabilities described above were not assessed during this evaluation. Only the functionality described in section 6 of this Security Target is considered to be within the logical boundary of the TOE.

The following figure depicts the TOE boundary.

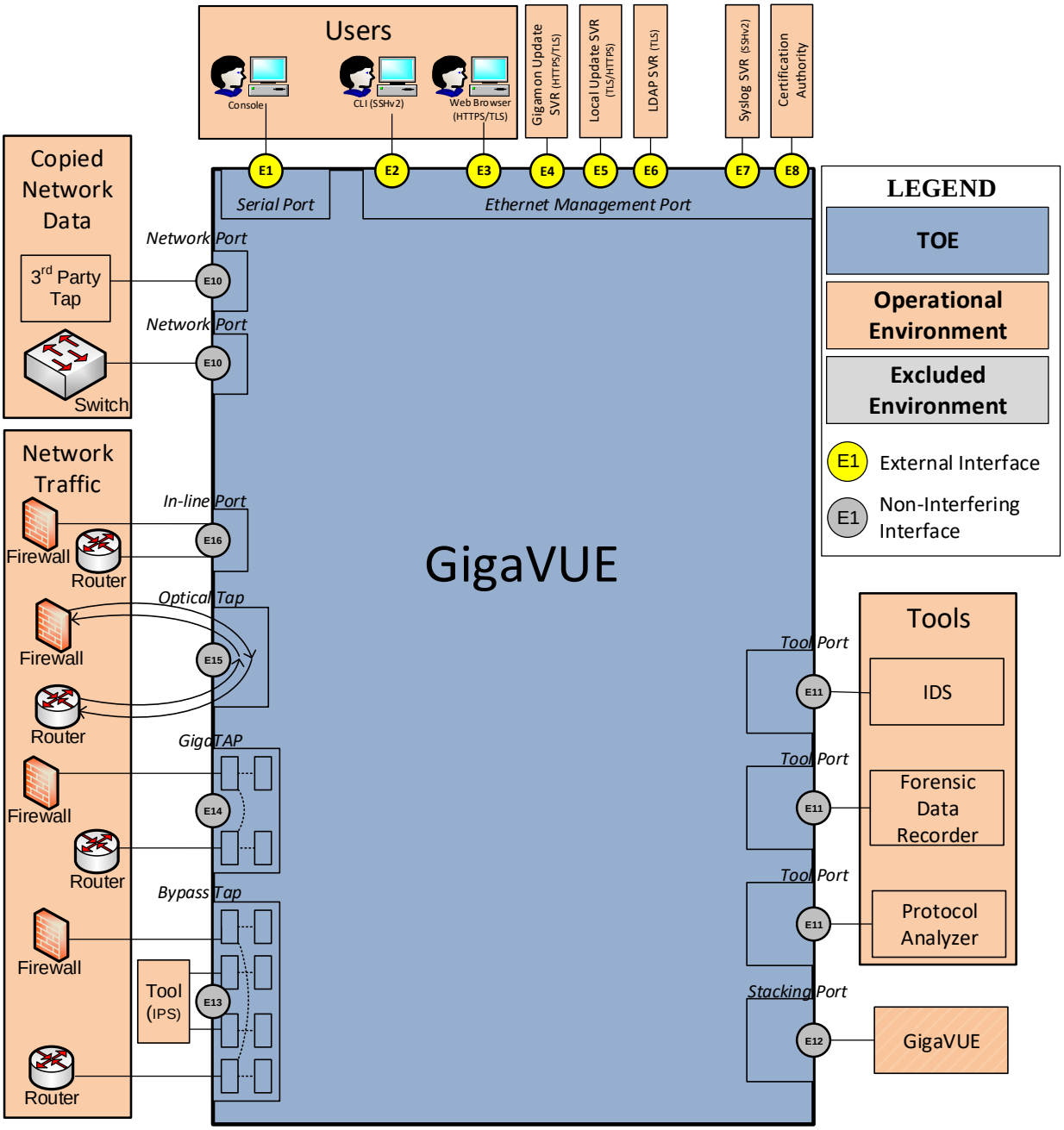

Figure 1: TOE Boundary for GigaVUE

As illustrated in Figure 1, the GigaVUE is a single hardware device that has management ports, network (or ingress) ports, and tool (or egress) ports. The external interfaces that are relevant to the TOE boundary are the local and remote administrative interfaces, an Update Server interface (whether maintained by Gigamon or residing in the local network), an LDAP server interface (for externally-defined I&A), and a Syslog Server interface (for external audit log storage). The TOE also interfaces with a Certification

Authority (CA) for issuance of server certificates and publication of a Certificate Revocation List (CRL) to determine the validity of certificates presented to the TOE.

1.4 TOE Type

The TOE type for this product is Network Device. The product is a hardware appliance whose primary functionality is related to the handling of network traffic. The NDcPP defines a network device as "a device composed of hardware and software that is connected to the network and has an infrastructure role within the network." The TOE is a network device composed of hardware and software that is connected to the network and accepts packets of data, filters them and passes them to tools for further analysis. The device's role in the enterprise network is to direct out-of-band network traffic for analysis by various tools, so its infrastructure role is self-evident.

2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes the physical and logical boundaries of the TOE.

2.1 Evaluated Components of the TOE

The following table describes the TOE components in the evaluated configuration:

Component	Definition
GigaVUE-HD8	14RU fabric node
GigaVUE-HD4	5RU fabric node
GigaVUE-HC3	3RU fabric node
GigaVUE-HC2	2RU fabric node
GigaVUE-HC1	1RU fabric node
GigaVUE-TA100	1RU traffic aggregator
GigaVUE-TA10	1RU traffic aggregator
GigaVUE-TA40	1RU edge node

Table 2-1: Evaluated Components of the TOE

2.2 Components and Applications in the Operational Environment

The following table lists components and applications in the TOE's operational environment that must be present for the TOE to be operating in its evaluated configuration:

Component	Definition
Certification Authority	A server that acts as a trusted issuer of digital certificates and distributes a CRL that identifies revoked certificates.
LDAP Server	A system that is capable of receiving authentication requests using LDAP over TLS and validating these requests against identity and credential data that is defined in an LDAP directory.
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client to access the CLI or a web browser (Microsoft Internet Explorer 11 or higher and Google Chrome 36 or higher) to access the web GUI, or

	locally, in which case the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications.
Syslog Server	The Syslog Server connects to the TOE and allows the TOE to send Syslog messages to it for remote storage. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
Update Server	A general-purpose computer that includes a web server and is used to store software update packages that can be retrieved by the TOE using TLS/HTTPS. The Update Server can be a server maintained by Gigamon or it can be set up locally in the Operational Environment by an administrator if the TOE's deployment prevents it from being able to access Gigamon's web domain.

Table 2-2: Evaluated Components of the Operational Environment

2.3 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with the TOE but are not included in the evaluated configuration. They provide no added security related functionality for the evaluated product. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

2.3.1 Not Installed

There are no optional components that are omitted from the installation process.

2.3.2 Installed but Requires a Separate License

There are no excluded components that are installed and require a separate license.

2.3.3 Installed but Not Part of the TSF

- **Insecure mode of operation** – GigaVUE provides an 'Secure Cryptography Mode' that restricts the cryptographic algorithms and ciphersuites to what is claimed in the Security Target. Operating the product outside of this mode of operation is not within the scope of the TSF
- **SCP/SFTP/FTP/TFTP mode of updating** – GigaVUE provides several methods to download product updates from the Operational Environment. In the evaluated configuration, only the TLS/HTTPS method of downloading is permitted, and the remaining methods are not part of the TOE.
- **TLS mode of syslog handling** – GigaVUE provides an additional method of off-loading the audit data using a TLS connection to the syslog server. In the evaluated configuration, only the SSH method of sending audit records is permitted and the remaining methods are not part of the TOE.
- **Port Blades, TAP Modules, Bypass Combo Modules and Port Modules** – Modular components of the GigaVUE used to capture traffic from the network in a variety of methods, for different scenarios, and to support different types of network media. GigaVUE's network traffic capture, filter, and forwarding capabilities were not assessed during this evaluation.

- **Stacking** – Combining multiple GigaVUE devices through a dedicated network port for the purpose of load balancing or to forward traffic received by one device to a tool connected to another device.
- **Telnet** – GigaVUE supports both Telnet and SSH2 for remote administration. In the evaluated configuration Telnet will be disabled.

Additionally, the TOE includes a number of functions that are outside the scope of the claimed Protection Profile. These functions are not part of the TSF because there are no SFRs that apply to them.

2.4 Physical Boundary

2.4.1 Hardware

GigaVUE is a rack-mounted hardware device. The GigaVUE is a modular device to accommodate many variations of physical connectivity including copper, fiber, 1G, 10G, 40G and 100G ports.

The model specific hardware and their configurations are as follows:

Property	HD8	HD4
Model Number	GVS-HD8A1 (AC power) GVS-HD8A2 (DC power)	GVS-HD4A1 (AC power) GVS-HD4A2 (DC power)
Size	14RU	5RU
Total Slots	8	5
Power	AC or DC	AC or DC
Control Cards	2 (10/100/1000M Mgmt. port Serial Console per Controller card)	1 (10/100/1000M Mgmt. port Serial Console per Controller Card)
Port Blades	PRT-H00-X12G04 Port Blade, 12x10Gb and 4x1Gb PRT-H00-X12TS Port Blade, H Series, 12x10G Time Stamp PRT-H00-X04G44 Port Blade, 4x10Gb and 32x10Gb PRT-H00-Q02X32 Port Blade, H Series, 2x40Gb and 32x10Gb PRT-HD0-Q08 Port Blade, H Series, 8x40Gb PRT-HD0-C06X24 Port Blade, HD Series, 6x100G QSFP28 cages + 24x10G cages PRT-HD0-C02X08 Port Blade, HD Series, 2x100G CFP cages + 8x10G cages PRT-HD0-C02X08A Port Blade, HD Series, 2x100G CFP2 cages + 8x10G cages	
Power Supplies	4	2
Processor	NXP QorIQ P2041	NXP QorIQ P2041
Fixed Ports	None	None
Configurable Ports	Provided by Port Blades	Provided by Port Blades

Table 2-3: HD Series Properties

Property	HC3	HC2	HC1
Model Number	GVS-HC301 (AC power)	GVS-HC2A1 (AC power)	GVS-HC101 (AC power)

	GVS-HC302 (DC power)	GVS-HC2A2 (DC power)	GVS-HC102 (DC power)
Size	3RU	2RU	1RU
TAP Modules	None	TAP-HC0-D25AC0 TAP module, SX/SR Internal TAP module 50/125, 12 TAPs TAP-HC0-D25BC0 TAP module, SX/SR Internal TAP module 62.5125, 12 TAPs TAP-HC0-D35CC0 TAP module, LX/LR Internal TAP module, 12 TAPs TAP-HC0-G100C0 TAP and Bypass Module, Copper, 12 TAP or BPS pairs	TAP-HC1-G10040 TAP and Bypass module, 10/100/1000M Copper, 4 TAPs or BPC pairs
Bypass Combo Modules	BPS-HC3-C25F26 Bypass Combo Module, GigaVUE-HC3, 2 100Gb SR4 BPS pairs, 16 10G cages	BPS-HC0-D25A4G Bypass Combo Module 4 SX/SR 50/125 BPS pairs, 16 10G cages BPS-HC0-D25B4G Bypass Combo Module 4 SX/SR 62.5/125 BPS pairs, 16 10G cages BPS-HC0-D35C4G Bypass Combo Module 4 LX/LR BPS pairs, 16 10G cages BPS-HC0-Q25A28 Bypass Combo Module 2 40G SR4 BPS pairs, 8 10G cages	BPS-HC1-D25A24 Bypass Combo Module, 2 SX/SR 50/125 BPS pairs, 4 10G cages
Smart Modules	SMT-HC3-C05 GigaSMART, GigaVUE-HC3, 5x100G QSFP28 cages (includes Slicing, Masking, Source Port, and GigaVUE Tunneling De-Encapsulation software)	SMT-HC0-R GigaSMART, GigaVUE-HC2 rear module (includes Slicing, Masking, Source Port, and GigaVUE Tunneling De-Encapsulation software) SMT-HC0-X16 GigaSMART, GigaVUE-HC2 front module, 16 10G cages (includes Slicing, Masking, Source Port, and GigaVUE Tunneling De-Encapsulation software)	None
Port Modules	PRT-HC3-C08Q08 Port Module, 8x100G QSFP28 cages, 8x40 QSFP+ cages	PRT-HC0-X24 Port Module, 24x10G (QSFP) PRT-HC0-Q06 Port Module, 6x40G (QSFP+)	None

	PRT-HC3-X24 Port Module, GigaVUE-HC3, 24x10G	PRT-HC0-C02 Port Module, 2x100G (QSFP28)	
Processor	Intel Atom C2758	NXP QorIQ P2041	Intel Atom C2358
Fixed Ports	10/100/1000M Mgmt. port Serial Console	10/100/1000M Mgmt. port Serial Console	10/100/1000M Mgmt. port Serial Console 12 1G/10G Ports (QSFP) 4 10/100/1000M Ports
Configurable Ports	Provided by Port Modules	Provided by TAP modules, Bypass Combo modules, Port Modules	Provided by TAP modules, Bypass Combo modules

Table 2-4: HC Series Properties

Property	TA10	TA40	TA100
Model Number	GigaVUE-TA10 Edge Traffic Aggregation Node GVS-TAX01 (AC power) GVS-TAX02 (DC power)	GigaVUE-TA40 Edge Traffic Aggregation Node GVS-TAQ01 (AC power) GVS-TAQ02 (DC power)	GigaVUE-TA100 Edge Traffic Aggregation Node GVS-TAC01 (AC power) GVS-TAC02 (DC power)
Size	1RU	1RU	1RU
Processor	NXP QorIQ P2020	NXP QorIQ P2020	Intel Atom C2338
Fixed Ports	10/100/1000M Mgmt. port Serial Console 48 1G/10G Ports (SFP+) 4 10G/40G QSFP Ports	10/100/1000M Mgmt. port Serial Console 32 10G/40G QSFP Ports	10/100/1000M Mgmt. port Serial Console 32 100GB QSFP28 ports
Configurable Ports	None	None	None

Table 2-5: TA Series Properties

2.4.2 Software

- Gigamon GigaVUE with software version 5.1.01.

Note that the GigaVUE software is built on top of the following CentOS versions.

GigaVUE OS	CentOS
HD4/HD8, HC2, TA10, TA40	CentOS 5.8
HC1, HC3, TA100	CentOS 6.6

Table 2-6: Software Versions

2.5 Logical Boundary

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

Security Audit

Cryptographic Support
Identification and Authentication
Security Management
Protection of the TSF
TOE Access
Trusted Path/Channels

2.5.1 Security Audit

Audit records are generated for various types of management activities and events. The audit records include the date and time stamp of the event, the event type and subject identity. In the evaluated configuration, the TSF is configured to transmit audit data to a remote Syslog Server using SSHv2, but audit data is also stored locally to ensure availability of the data if communications with the Syslog Server are unavailable. Local audit records are stored in "message" files which are rotated to ensure a maximum limit of disk usage is enforced. Only users with the Admin privilege can access or delete the log files. Users with the Admin privilege are considered trusted users and are therefore not expected to delete or modify the audit records.

2.5.2 Cryptographic Support

The TOE uses sufficient security measures to protect its data in transmission by implementing cryptographic methods and trusted channels. The TOE uses SSH to secure the remote CLI and Syslog Server trusted channels. The TOE also uses TLS/HTTPS to secure the trusted channels for the secure web GUI, Update Server and LDAP server. SSH communications are established using Diffie-Hellman group 14 while TLS communications are established using the ECC scheme using NIST curve P-256.

Cryptographic keys are generated using the CTR_DRBG provided by this module. The TOE erases all plaintext secret and private keys that reside in both RAM and non-volatile storage with zeroes. In the evaluated configuration, the TOE operates in "Secure Cryptography Mode" which is used to restrict algorithms to meet the PP requirements.

The following table contains the CAVP algorithm certificates:

SFR	Algorithm	CAVP Cert. #
FCS_CKM.1 FCS_COP.1/SigGen	ECDSA	#1492
FCS_CKM.2	CVL	#1981
FCS_COP.1/DataEncryption	AES	#5541
FCS_COP.1/Hash	SHS	#4447
FCS_COP.1/KeyedHash	HMAC	#3692
FCS_RBG_EXT.1	DRBG	#2196

Table 2-7: Cryptographic Algorithm Table

2.5.3 Identification and Authentication

All users must be identified and authenticated to the TOE before being allowed to perform any actions on the TOE. This is true of users accessing the TOE via the local console, or protected paths using the remote CLI via SSH or web GUI via TLS/HTTPS. Users authenticate to the TOE using one of the following methods:

- Username/password (defined on the TOE)
- LDAP authentication
- Username/public key (SSH only)

The TSF provides a configurable number of maximum consecutive authentication failures that are permitted by a user. Once this number has been met, the account is locked for a configurable time interval. Passwords that are maintained by the TSF can be composed of upper case, lower case, numbers and special characters. The Security Administrator can define the password length between 8 and 30 characters. Password information is never revealed during the authentication process including during login failures. Before a user authenticates to the device, a configurable warning banner is displayed.

As part of establishing trusted remote communications, the TOE provides X.509 certificate functionality. In addition to verifying the validity of certificates, the TSF can check their revocation status using a certificate revocation list (CRL). The TSF can also generate a Certificate Signing Request in order to obtain a signed certificate to install for its own use as a TLS server.

2.5.4 Security Management

The TOE defines two roles: Admin and Monitor. Each of these roles has varying levels of fixed privilege to interact with the TSF. The Admin role is able to perform all security-relevant management functionality (such as user management, password policy configuration, application of software updates, and configuration of cryptographic settings). The Monitor role provides view-only access to ports and configurations. Therefore, the term “Admin”, used throughout this document, is considered to be a Security Administrator of the TSF. Management functions can be performed using the local CLI, remote CLI, or web GUI. All software updates to the TOE are performed manually.

2.5.5 Protection of the TSF

The TOE stores usernames and passwords in a password file that cannot be viewed by any user on the TOE regardless of the user's role. The passwords are hashed using SHA-512. Public keys are stored in the configuration database which is integrity checked at boot time. Key data is stored in plaintext on the hard drive but cannot be accessed by any user. The TOE has an underlying hardware clock that is used for keeping time. The time can be manually set by the administrator. Power-on self-tests are executed automatically when the FIPS validated cryptographic module is loaded into memory. The FIPS cryptographic module verifies its own integrity using an HMAC-SHA1 digest computed at build time. All binaries (e.g. executables, libraries), are located on a read-only partition and cannot be modified. In addition, the TOE has a configuration database that is integrity checked at boot time.

The version of the TOE (both the currently executing version and the installed/updated version, if different) can be verified from any of the administrative interfaces provided by the TSF. The TOE is updated via the Gigamon Update Server or the local Update Server via an HTTPS protected connection. The updated image is verified via a digital signature.

2.5.6 TOE Access

The TOE can terminate inactive local console, remote CLI or web GUI sessions after a specified time period. The default setting is 15 minutes. Users can also terminate their own interactive sessions. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session. The

TOE displays an administratively configured banner on the local console or remote CLI and the web GUI prior to allowing any administrative access to the TOE.

2.5.7 Trusted Path/Channels

The TOE connects and sends data to IT entities that reside in the Operational Environment via trusted channels. In the evaluated configuration, the TOE connects with a Syslog Server using SSH to encrypt the audit data that traverses the channel. The TOE also connects with an LDAP server using TLS and to an Update Server using TLS/HTTPS. The Update Server may either be one maintained by Gigamon, or a local server that is deployed in the TOE's Operational Environment. When accessing the TOE remotely, administrators interface with the TSF using a trusted path. The remote CLI is protected via SSH and the web GUI is protected by TLS/HTTPS.

3 Conformance Claims

3.1 CC Version

This ST is compliant with Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 September 2012.

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 extended to include all applicable NIAP and International interpretations through August 21, 2018.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) are conformant to Part 3 to include all applicable NIAP and International interpretations through August 21, 2018.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profiles:

- collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314 [NDcPP]
- The following is the list of NIAP Technical Decisions that are applicable to the ST/TOE and a summary of their impact:

		Changes			Analysis to this evaluation	
TD #	Title	SFR	AA	Notes	NA	Reason
TD0343	NIT Technical Decision for Updating FCS_IPSEC_EXT.1.14 Tests	X	X			Not claiming IPSEC
TD0342	NIT Technical Decision for TLS and DTLS Server Tests		X			

TD0341	NIT Technical Decision for TLS wildcard checking			X		
TD0340	NIT Technical Decision for Handling of the basicConstraints extension in CA and leaf certificates	X				
TD0339	NIT Technical Decision for Making password-based authentication optional in FCS_SSHS_EXT.1.2	X	X	X		
TD0338	NIT Technical Decision for Access Banner Verification		X			
TD0337	NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6	X	X	X		
TD0336	NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8		X			
TD0335	NIT Technical Decision for FCS_DTLS Mandatory Cipher Suites			X		Not claiming DTLS but claiming TLSS. The TD references TLSS but has not authorized changes to the TLSS application note.
TD0334	NIT Technical Decision for Testing SSH when password-based authentication is not supported		X			
TD0333	NIT Technical Decision for Applicability of FIA_X509_EXT.3	X	X	X		
TD0324	NIT Technical Decision for Correction of section numbers in SD Table 1		X		X	No change to ST, identifies a change in a table in the SD.
TD0323	NIT Technical Decision for DTLS server testing - Empty Certificate Authorities list		X		X	No change to ST, not claiming DTLS.
TD0322	NIT Technical Decision for TLS server testing - Empty Certificate Authorities list		X		X	No change to ST.
TD0321	Protection of NTP communications			X		No change to ST.
TD0291	NIT technical decision for DH14 and FCS_CKM.1	X				Change to the text of FCS_CKM.1.1.
TD0290	NIT technical decision for physical interruption of trusted path/channel.		X			No change to ST, TD specifies how its trusted channel functionality is tested.
TD0289	NIT technical decision for FCS_TLSC_EXT.x.1 Test 5e		X		X	No change to ST, TD specifies how its claimed TLS client functionality is tested.
TD0281	NIT Technical Decision for Testing both thresholds for SSH rekey		X			No change to ST, TD specifies how its claimed TLS server functionality is tested.
TD0260	NIT Technical Decision for Typo in FCS_SSHS_EXT.1.4	X				Grammatical change to the text of FCS_SSHS_EXT.1.4.
TD0259	NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187	X		X		Change to the text of FCS_SSHC_EXT.1.5 and FCS_SSHS_EXT.1.5.

TD0257	NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4		X		X	No change to ST, TD specifies how its claimed TLS client functionality is tested.
TD0256	NIT Technical Decision for Handling of TLS connections with and without mutual authentication		X		X	No change to ST, TD specifies how its claimed TLS client functionality is tested.
TD0228	NIT Technical Decision for CA certificates - basicConstraints validation		X		X	No change to ST, TD specifies how its claimed X.509 functionality is tested.

Table 3-1: Technical Decisions

Note that Technical Decisions were not considered to be applicable if any of the following conditions were true:

- The Technical Decision does not apply to the NDcPP.
- The Technical Decision does not apply to the current version of the NDcPP.
- The Technical Decision applies to an SFR that was not claimed by the TOE.
- The Technical Decision applies to an SFR selection or assignment that was not chosen for the TOE.
- The Technical Decision only applies to one or more Application Notes in the NDcPP and does not affect the SFRs or how the evaluation of the TOE is conducted.
- The Technical Decision is an affirmation that an existing requirement or Evaluation Activity is correct.
- The Technical Decision was superseded by a more recent Technical Decision.
- The Technical Decision is issued as guidance for future versions of the NDcPP.

3.5 Package Claims

The TOE claims exact conformance to the NDcPP, which is conformant with CC Part 3.

The TOE claims following Selection-Based SFRs that are defined in the appendices of the claimed PP:

- FCS_HTTPS_EXT.1
- FCS_SSHC_EXT.1
- FCS_SSHS_EXT.1
- FCS_TLSC_EXT.1
- FCS_TLSS_EXT.1
- FIA_X509_EXT.1/Rev
- FIA_X509_EXT.2
- FIA_X509_EXT.3

The TOE claims the following Optional SFRs that are defined in the appendices of the claimed PP:

- FAU_STG.1
- FMT_MTD.1/CryptoKeys

This does not violate the notion of exact conformance because the cPP specifically indicates these as allowable selections and options and provides both the ST author and evaluation laboratory with instructions on how these claims are to be documented and evaluated.

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are in exact conformance with the NDcPP.

3.7 Conformance Claim Rationale

The NDcPP states the following: “This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device… A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure within the network… Examples of network devices that are covered by requirements in this cPP include routers, firewalls, VPN gateways, IDSs, and switches.”

The TOE is a network device composed of hardware and software that is designed to apply forwarding rules to different types of network traffic so that it can be analyzed by a variety of third-party tools. As such, it can be understood as having a role in network infrastructure. Therefore, the conformance claim is appropriate.

4 Security Problem Definition

4.1 Threats

This section identifies the threats against the TOE. These threats have been taken from the NDcPP.

Threat	Threat Definition
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 includes 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	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

Table 4-1: TOE Threats

4.2 Organizational Security Policies

This section identifies the organizational security policies which are expected to be implemented by an organization that deploys the TOE. These policies have been taken from the NDcPP.

Policy	Policy Definition
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.

Table 4-2: Organizational Security Policies

4.3 Assumptions

The specific conditions listed in this section are assumed to exist in the TOE's Operational Environment. These assumptions have been taken from the NDcPP.

Assumption	Assumption Definition
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. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.

A.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 a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_ PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
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.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 4-3: TOE Assumptions

4.4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.4.1 TOE Security Objectives

The NDcPP does not define any security objectives for the TOE.

4.4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives:

Objective	Objective Definition
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_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.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.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
OE.TRUSTED_ADMIN	Security 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.

Table 4-4: Operational Environment Objectives

4.5 Security Problem Definition Rationale

The assumptions, threats, OSPs, and objectives that are defined in this ST represent the assumptions, threats, OSPs, and objectives that are specified in the Protection Profile to which the TOE claims conformance.

5 Extended Components Definition

5.1 Extended Security Functional Requirements

The extended Security Functional Requirements that are claimed in this ST are taken directly from the PP to which the ST and TOE claim conformance. These extended components are formally defined in the PP in which their usage is required.

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

6 Security Functional Requirements

6.1 Conventions

The CC permits four functional component operations—assignment, refinement, selection, and iteration—to be performed on functional requirements. This ST will highlight the operations in the following manner:

- **Assignment:** allows the specification of an identified parameter. Indicated with *italicized* text.
- **Refinement:** allows the addition of details. Indicated with **bold** text. Note that conversion of British spelling to American spelling is not marked as a refinement (e.g. 'authorisation' changed to 'authorization').
- **Selection:** allows the specification of one or more elements from a list. Indicated with underlined text.
- **Iteration:** allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR and/or separated by a "/" with a notation that references the function for which the iteration is used, e.g. "/TrustedUpdate" for an SFR that relates to update functionality

When multiple operations are combined, such as an assignment that is provided as an option within a selection or refinement, a combination of the text formatting is used.

If SFR text is reproduced verbatim from text that was formatted in a claimed PP (such as if the PP's instantiation of the SFR has a refinement or a completed assignment), the formatting is not preserved. This is so that the reader can identify the operations that are performed by the ST author as opposed to the PP author.

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

Class Name	Component Identification	Component Name
Security Audit (FAU)	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG_EXT.1	Protected Audit Event Storage
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_HTTPS_EXT.1	HTTPS Protocol
	FCS_RBG_EXT.1	Random Bit Generation

Class Name	Component Identification	Component Name
	FCS_SSHC_EXT.1	SSH Client Protocol
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSC_EXT.1	TLS Server Protocol
	FCS_TLSS_EXT.1	TLS Server Protocol
Identification and Authentication (FIA)	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_X509_EXT.1/Rev	X509 Certificate Validation
	FIA_X509_EXT.2	X509 Certificate Authentication
	FIA_X509_EXT.3	X509 Certificate Requests
Security Management (FMT)	FMT_MOF.1/ManualUpdate	Management of Security Functions Behavior
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
Protection of the TSF (FPT)	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Trusted Update
TOE Access (FTA)	FTA_SSL_EXT.1	TSF-Initiated Session Locking
	FTA_SSL.3	TSF-Initiated Termination
	FTA_SSL.4	User-Initiated Termination
	FTA_TAB.1	Default TOE Access Banners
Trusted Path/Channels (FTP)	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1/Admin	Trusted Path

Table 6-1: Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 Class FAU: Security Audit

6.3.1.1 *FAU_GEN.1 Audit Data Generation*

FAU_GEN.1.1

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

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising:
    - Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).

- Changes to TSF data related to 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).
- [no other actions]*;*

d) Specifically defined auditable events listed in Table **15**;

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 **15**.

Requirement	Auditable Event(s)	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG.1	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS session.	Reason for failure.
FCS_RBG_EXT.1	None.	None.
FCS_SSHC_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_TLSC_EXT.1	Failure to establish a TLS session.	Reason for failure.
FCS_TLSS_EXT.1	Failure to establish a TLS session.	Reason for failure.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP Address).
FIA_PMG_EXT.1	None.	None.
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP Address).
FIA_UAU.7	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP Address).
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate.	Reason for failure.
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None.
FMT_MTD.1/CoreData	All management activities of TSF data.	None.

FMT_MTD.1/CryptoKeys	Management of cryptographic keys.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_SSL_EXT.1	The termination of a remote session by the session locking mechanism.	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/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.

Table 6-2: Auditable Events

6.3.1.2 *FAU_GEN.2 User Identity Association*

FAU_GEN.2.1

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

6.3.1.3 *FAU_STG.1 Protected Audit Trail Storage*

FAU_STG.1.1

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

FAU_STG.1.2

The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

6.3.1.4 *FAU_STG_EXT.1 Protected Audit Event Storage*

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: [*delete the oldest compressed message file, increment the number of all other compressed message files, and create a new message file*]] when the local storage space for audit data is full.

6.3.2 Class FCS: Cryptographic Support

6.3.2.1 *FCS_CKM.1 Cryptographic Key Generation*

FCS_CKM.1.1[1]

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- ECC schemes using "NIST curves" [P-256] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;
- FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3].

6.3.2.2 *FCS_CKM.2 Cryptographic Key Establishment*

FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- Key establishment scheme using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3].

6.3.2.3 *FCS_CKM.4 Cryptographic Key Destruction*

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 [
    - logically addresses the storage location of the key and performs a [single-pass] overwrite consisting of [zeroes]]]

[1] TD0291

that meets the following: No Standard.

6.3.2.4 *FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)*

FCS_COP.1.1/DataEncryption

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].

6.3.2.5 *FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)*

FCS_COP.1.1/SigGen

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [*256 bit*]

that meet the following: [

- For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256]; ISO/IEC 14888-3, Section 6.4].

6.3.2.6 *FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)*

FCS_COP.1.1/Hash

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-512] and message digest sizes [160, 256, 512] bits that meet the following: ISO/IEC 10118-3:2004.

6.3.2.7 *FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)*

FCS_COP.1.1/KeyedHash

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512] and cryptographic key sizes [*160 bits, 256 bits, 512 bits*], and message digest sizes [160, 256, 512] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".

6.3.2.8 *FCS_HTTPS_EXT.1 HTTPS Protocol*

FCS_HTTPS_EXT.1.1

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

FCS_HTTPS_EXT.1.2

The TSF shall implement the HTTPS using TLS.

FCS_HTTPS_EXT.1.3

If a peer certificate is presented, the TSF shall [not require client authentication] if the peer certificate is deemed invalid.

6.3.2.9 *FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)*

FCS_RBG_EXT.1.1

The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*2*] software-based noise source**s**] 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 CSPs that it will generate.

6.3.2.10 *FCS_SSHC_EXT.1 SSH Client Protocol*

FCS_SSHC_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFCs [4251, 4252, 4253, 4254, 5656, 6668].

FCS_SSHC_EXT.1.2

The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [no other method].

FCS_SSHC_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [*65,535*] bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4[2]

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc].

FCS_SSHC_EXT.1.5[3]

The TSF shall ensure that the SSH public-key based authentication implementation uses [ecdsa-sha2-nistp256] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6[4]

The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256, hmac-sha2-512] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7

[2] TD0337
[3] TD0259
[4] TD0337

The 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

The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

FCS_SSHC_EXT.1.9

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 **and** [no other methods] as described in RFC 4251 section 4.1.

6.3.2.11 *FCS_SSHS_EXT.1 SSH Server Protocol*

FCS_SSHS_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFCs [4251, 4252, 4253, 4254, 5656, 6668].

FCS_SSHS_EXT.1.2[5]

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

FCS_SSHS_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [*65,535*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4[6]

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc].

FCS_SSHS_EXT.1.5[7]

The TSF shall ensure that the SSH public-key based authentication implementation uses [ecdsa-sha2-nistp256] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6[8]

The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256, hmac-sha2-512] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7

[5] TD0339
[6] TD0260 & TD0337
[7] TD0259
[8] TD0337

The 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

The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

6.3.2.12 *FCS_TLSC_EXT.1 TLS Client Protocol*

FCS_TLSC_EXT.1.1

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

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289].

FCS_TLSC_EXT.1.2

The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125 section 6.

FCS_TLSC_EXT.1.3

The TSF shall only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall [not establish the connection].

FCS_TLSC_EXT.1.4

The TSF shall [present the Supported Elliptic Curves Extension with the following NIST curves: [secp256r1] and no other curves] in the Client Hello.

6.3.2.13 *FCS_TLSS_EXT.1 TLS Server Protocol*

FCS_TLSS_EXT.1.1

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

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289]

FCS_TLSS_EXT.1.2

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

FCS_TLSS_EXT.1.3

The TSF shall [generate EC Diffie-Hellman parameters over NIST curves [secp256r1] and no other curves]

.

6.3.3 Class FIA: Identification and Authentication

6.3.3.1 *FIA_AFL.1 Authentication Failure Management*

FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within [*1 to 4,294,967,296*] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending remote Administrator from successfully authenticating until an Administrator defined time period has elapsed].

6.3.3.2 *FIA_PMG_EXT.1 Password Management*

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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”];
b) Minimum password length shall be configurable **from** [*8 characters*] **to** [*30 characters*].

6.3.3.3 *FIA_UAU_EXT.2 Password-Based Authentication Mechanism*

FIA_UAU_EXT.2.1

The TSF shall provide a local password-based authentication mechanism and [[*an LDAP authentication mechanism, an SSH public-key based authentication mechanism*]] to perform local administrative user authentication.

6.3.3.4 *FIA_UAU.7 Protected Authentication Feedback*

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.

6.3.3.5 *FIA_UIA_EXT.1 User Identification and Authentication*

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.

6.3.3.6 *FIA_X509_EXT.1/Rev X.509 Certificate Validation*

FIA_X509_EXT.1.1/Rev[9]

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

- RFC 5280 certificate validation and certificate path validation supporting a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3].
- 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.

FIA_X509_EXT.1.2/Rev

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.

6.3.3.7 *FIA_X509_EXT.2 X.509 Certificate Authentication*

FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS, HTTPS], and [no additional uses].

FIA_X509_EXT.2.2

[9] TD0340

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

6.3.3.8 *FIA_X509_EXT.3 X.509 Certificate Requests*

FIA_X509_EXT.3.1[10]

The TSF shall generate a Certificate Request as specified by RFC 2986 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.

6.3.4 Class FMT: Security Management

6.3.4.1 *FMT_MOF.1/ManualUpdate Management of Security Functions Behavior*

FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions to perform manual update to Security Administrators.

6.3.4.2 *FMT_MTD.1/CoreData Management of TSF Data*

FMT_MTD.1.1/CoreData

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

6.3.4.3 *FMT_MTD.1/CryptoKeys Management of TSF Data*

FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

6.3.4.4 *FMT_SMF.1 Specification of Management Functions*

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 [digital signature] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;

[10] TD0333

- [Ability to configure the cryptographic functionality;
- Ability to set the time which is used for time-stamps].

Application Note: *The list of management functions is marked as assignments in the NDcPP but have been formatted as selections here because the operations are defined as literal text that must be chosen as opposed to open-ended prompts to be completed by the ST author.*

6.3.4.5 *FMT_SMR.2 Restrictions on Security Roles*

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

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

are satisfied.

6.3.5 Class FPT: Protection of the TSF

6.3.5.1 *FPT_APW_EXT.1 Protection of Administrator Passwords*

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.

6.3.5.2 *FPT_SKP_EXT.1 Protection of TSF Data (For Reading of All Pre-shared, Symmetric and Private Keys)*

FPT_SKP_EXT.1.1

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

6.3.5.3 *FPT_STM_EXT.1 Reliable Time Stamps*

FPT_STM_EXT.1.1

The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2

The TSF shall [allow the Security Administrator to set the time].

6.3.5.4 *FPT_TST_EXT.1 TSF Testing*

FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [during initial start-up (on power on), [*continuously*]] to demonstrate the correct operation of the TSF: [*software integrity, cryptographic module integrity, hardware integrity, continuous RNG test*].

6.3.5.5 *FPT_TUD_EXT.1 Trusted Update*

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 [digital signature mechanism] prior to installing those updates.

6.3.6 Class FTA: TOE Access

6.3.6.1 *FTA_SSL_EXT.1 TSF-initiated Session Locking*

FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions,

- [terminate the session]

after a Security Administrator-specified time period of inactivity.

6.3.6.2 *FTA_SSL.3 TSF-initiated Termination*

FTA_SSL.3.1

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

6.3.6.3 *FTA_SSL.4 User-initiated Termination*

FTA_SSL.4.1

The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

6.3.6.4 *FTA_TAB.1 TOE Access Banner*

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.

6.3.7 Class FTP: Trusted Path/Channels

6.3.7.1 *FTP_ITC.1 Inter-TSF Trusted Channel*

FTP_ITC.1.1

The TSF shall be capable of using [SSH, TLS, HTTPS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [authentication server, [*Update 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 [*authentication requests, transferring audit records, downloading software updates*].

6.3.7.2 *FTP_TRP.1/Admin Trusted Path*

FTP_TRP.1.1/Admin

The TSF shall be capable of using [SSH, TLS, HTTPS] 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/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

FTP_TRP.1.3/Admin

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

6.4 Statement of Security Functional Requirements Consistency

The Security Functional Requirements included in the ST represent all required SFRs specified in the claimed PP, a subset of the optional requirements, and all applicable selection-based requirements that have been included as specified for the claimed PP.

7 Security Assurance Requirements

This section identifies the Security Assurance Requirements (SARs) that are claimed for the TOE. The SARs which are claimed are in exact conformance with the NDcPP.

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 *Developer action elements:*

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

The developer shall provide a tracing from the functional specification to the SFRs.

7.1.1.2 *Content and presentation elements:*

ADV_FSP.1.1C

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

7.1.1.3 *Evaluator action elements:*

ADV_ FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_ FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

7.2 Class AGD: Guidance Documentation

7.2.1 Operational User Guidance (AGD_OPE.1)

7.2.1.1 *Developer action elements:*

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 *Content and presentation elements:*

AGD_OPE.1.1C

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.2.1.3 *Evaluator action elements:*

AGD_OPE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.2.2 Preparative Procedures (AGD_PRE.1)

7.2.2.1 *Developer action elements:*

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.2.2.2 *Content and presentation elements:*

AGD_ PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

7.2.2.3 *Evaluator action elements:*

AGD_ PRE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

7.3 Class ALC: Life Cycle Supports

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 *Developer action elements:*

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

7.3.1.2 *Content and presentation elements:*

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 *Evaluator action elements:*

ALC_CMC.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.3.2 TOE CM Coverage (ALC_CMS.1)

7.3.2.1 *Developer action elements:*

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.3.2.2 *Content and presentation elements:*

ALC_CMS.1.1C

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

7.3.2.3 *Evaluator action elements:*

ALC_CMS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.4 Class ATE: Tests

7.4.1 Independent Testing - Conformance (ATE_IND.1)

7.4.1.1 *Developer action elements:*

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.4.1.2 *Content and presentation elements:*

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 *Evaluator action elements:*

ATE_IND.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

7.5 Class AVA: Vulnerability Assessment

7.5.1 Vulnerability Survey (AVA_VAN.1)

7.5.1.1 *Developer action elements:*

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 *Content and presentation elements:*

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 *Evaluator action elements:*

AVA_VAN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

8 TOE Summary Specification

The following sections identify the security functions of the TOE and describe how the TSF meets each claimed SFR. They include Security Audit, Cryptographic Support, Identification and Authentication, Security Management, Protection of the TSF, TOE Access, and Trusted Path/Channels.

8.1 Security Audit

8.1.1 FAU_GEN.1:

The TOE contains mechanisms to generate audit data based upon successful and unsuccessful management actions by all authorized users of the TOE. Each audit record contains identifying information of the subject performing the action. The audit records are generated and stored in the form of syslog records which are sent securely to the Syslog Server protected by SSHv2. The TOE maintains log levels which determine the set of events that are logged. The log level is set using the following command: `logging level`. Setting the log-level to "info" captures all the necessary logs defined in the NDcPP.

The TOE allows viewing of the audit records through the local console with the following command: `show log`. Users of any role can view audit log files, however, only Admin users can delete audit log files. If an Admin deletes a log file, an audit record of that action is also recorded.

Table 9-1 in Appendix A lists the auditable events defined by this component and examples of audit records for that particular event.

The audit records that the TOE creates include the following information: date and time of the event, event type, subject identity, success or failure of the event, and source of the event.

8.1.2 FAU_GEN.2:

The TOE records the identity of the user (e.g. username, system name, IP address) associated with each audited event in the audit record.

8.1.3 FAU_STG.1:

The TOE allows viewing of the audit records through the CLI with the following command: `show log`. Users of any role can view audit log files, however, only Admin users can delete audit log files. No modification of log files is permitted, regardless of role. If an Admin deletes a log file, an audit record of that action is also recorded. The TOE allocates up to 8MB for the audit log but rolls this data over to a backup file and compresses it once full. A maximum of 8 backup files exist, and the oldest one is deleted as part of a rollover process when a new backup is created.

8.1.4 FAU_STG_EXT.1:

In the evaluated configuration, the TOE will send audit records to a remote Syslog Server via an encrypted SSH channel over the Ethernet Management Port. When the Syslog Server is configured, the audit records are stored locally and immediately pushed to the Syslog Server. If Syslog Server connectivity is unavailable, audit records will only be stored locally. Upon re-establishment of communications with the Syslog Server, new audit records will resume being transmitted to it but the

audit records that were generated during the time the Syslog Server connection was down remain stored locally and are not sent to the Syslog Server.

New audit records are stored locally on the TOE under the /var/log directory in the file named “messages". The "message" file is archived when it reaches a specific size (8MB) by compressing it and saving the file as "messages.1.gz”. Meanwhile, a new "messages" file is created for new audit records and the other compressed messages files are rotated so that the 8 most recent compressed messages files are saved. The 8 compressed files are named "messages.1.gz”, “messages2.gz”, and so on. Therefore, as part of the file rotation “messages8.gz” will be deleted, "messages.7.gz" will be saved as "messages.8.gz", "messages.6.gz" will be saved as "messages.7.gz", and so on until the "messages" file is compressed into "messages.1.gz”. This mechanism guarantees a maximum limit of disk usage used by the log files. Only a user with the Admin role can delete the log files. Users with the Admin role are considered trusted users and are not expected to delete the audit records.

8.2 Cryptographic Support

8.2.1 **FCS_CKM.1:**

The TOE generates ECC keys using NIST curve P-256, in accordance with FIPS PUB 186-4. The ECC keys are generated in support of device authentication. Also, the TOE uses finite field cryptography (FFC) Diffie-Hellman group 14 key with key size of 2048 bits that meet the following: RFC 3526 Section 3. These keys are used for SSH and TLS key establishment.

The TOE’s key generation function is validated under CAVP ECDSA certificate: #1492.

8.2.2 **FCS_CKM.2:**

The TOE implements NIST SP 800-56A Revision 2 conformant key establishment mechanisms for Elliptic Curve Diffie-Hellman (ECDH) key establishment schemes. Specifically, the TOE complies with the NIST SP 800-56A Revision 2 key agreement scheme (KAS) primitives that are defined in section 5.6 of the SP. This is used for the establishment of TLS sessions, for which the TOE can act as both a sender and a receiver.

In addition, the TOE implements Diffie-Hellman group 14 with key size of 2048 bits for SSH key establishment, for which the TOE can also be both a sender and a receiver. The group, prime, hexadecimal value, and generator are all consistent with RFC 3526, section 3.

The TOE’s implementation of NIST SP 800-56A Revision 2 is validated under CAVP CVL certificate #1981.

8.2.3 **FCS_CKM.4:**

The TOE implements secure key destruction as follows:

- Keys stored in volatile memory: These keys are immediately zeroized using the function memset() upon deallocation. These keys are destroyed when sessions are closed.
- Keys stored in non-volatile memory: The TOE zeroizes all plaintext secret and private cryptographic keys in persistent storage by overwriting the file with zeroes and performing a read verify. Upon successful completion of the zeroization, the file is deallocated using the

file system API unlink(). These keys are destroyed during import/re-installation or upgrade/regeneration.

The TOE is not subject to any situations that would prevent or delay key destruction and strictly conforms to the key destruction requirements. This combined approach protects the keys in volatile and non-volatile memory from being compromised. The following table identifies the 0keys and CSPs that are applicable to the TOE as well as their usage, storage location, and method of destruction:

Key Material	Origin	Storage Location	Clearing of Key Material
SSH keys	SSH server/ client application	Non-volatile storage/file system	Upon regeneration of keys.
Authentication keys	X.509 certificates	Non-volatile storage/ file system	Upon import/creation of configuration DB on installation or upgrade.
TLS session keys	syslogtls, radsec applications	RAM Non-volatile storage	For RAM: Destroyed on close of session For non-volatile storage, Upon regeneration of keys.

Table 8-1: Cryptographic Materials, Storage, and Destruction Methods

8.2.4 FCS_COP.1/DataEncryption:

The TOE performs encryption and decryption using the AES algorithm in CBC mode with key sizes of 128 and 256 bits. This algorithm implementation is validated under CAVP AES certificate #5541. The AES algorithm meets ISO/IEC 18033-3 and the CBC mode implementation meets ISO/IEC 10116.

8.2.5 FCS_COP.1/SigGen:

The TOE performs signature generation and validation using Elliptic Curve Digital Signature Algorithm (ECDSA). The TOE supports ECDSA with 256 bit key size and implements the NIST P-256 curve. The ECDSA implementation meets ISO/IEC 14888-3 Section 6.4 and FIPS 186-4. This implementation is validated under CAVP ECSDA certificate #1492.

8.2.6 FCS_COP.1/Hash:

The TOE provides cryptographic hashing services using SHA-1, SHA-256, and SHA-512 with message digest sizes of 160, 256, and 512 bits respectively, as specified in FIPS PUB 186-4. The TSF uses hashing services the following functions:

- SHA-1, SHA-256, and SHA-512 for SSH data integrity
- SHA-1 for software integrity
- SHA-1 for TLS
- SHA-1 for digital signature
- SHA-512 for password hashing

The SHA algorithm meets ISO/IEC 10118-3:2004 and is validated under CAVP SHS certificate #4447.

8.2.7 FCS_COP.1/KeyedHash:

The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512. The HMAC implementation supports key sizes that are equal to block sizes. HMAC is implemented as specified in FIPS PUB 198-1 and FIPS PUB 180-3, and the following MAC sizes are supported:

- HMAC-SHA-1: 10, 12, 16, 20 bytes.
- HMAC-SHA-256: 16, 24, 32 bytes.
- HMAC-SHA-512: 32, 40, 48, 56, 64 bytes.

The algorithm meets ISO/IEC 9797-2:2011 Section 7 and is validated under CAVP HMAC certificate #3692.

8.2.8 FCS_HTTPS_EXT.1:

The TOE implements HTTPS in order to facilitate remote administration over the web GUI and to download software updates from an HTTPS server in the Operational Environment. The HTTPS implementation conforms to RFC 2818 and uses the TLS client/server implementations specified in FCS_TLSC_EXT.1 and FCS_TLSS_EXT.1. Since the HTTPS server does not enforce TLS mutual authentication, the only prerequisite to establishment of a TLS connection is that the peer initiate the communications.

8.2.9 FCS_RBG_EXT.1:

The TOE implements a NIST-approved deterministic random bit generator (DRBG). The DRBG used by the TOE is the CTR_DRBG with AES as specified by ISO/IEC 18031:2011. The TOE models uniformly provide two software-based entropy sources as described in the proprietary entropy specification. The DRBG is seeded with a minimum of 256 bits of entropy so that it is sufficient to ensure full entropy for 256-bit keys, which are the largest keys generated by the TSF. The TOE's DRBG implementation meets ISO/IEC 18031:2011 and is validated under CAVP certificate #2196.

8.2.10 FCS_SSHC_EXT.1/ FCS_SSHS_EXT.1:

SSHv2 is used to secure the remote CLI management connection (SSH Server) and Syslog connection (SSH Client) between the TOE and a remote Syslog Server The traffic for both of these connections is sent via the Ethernet Management Port and by default, the SSHv2 port used is port 22.

The TOE implements the SSHv2 protocol that complies with the following RFCs: 4251, 4252, 4253, 4254, 5656, and 6668. The TOE supports password based and public key based authentication methods as described in RFC 4252; both authentication methods are supported on the remote CLI but only public key based authentication is used when communicating with the remote Syslog Server. The TOE implements public key authentication using ecdsa-sha2-nistp256. Per RFC 4251 section 4.1, the TOE's SSH client implementation will authenticate the identity of the Syslog Server (i.e. SSH server) by using its local database (i.e. /.ssh/knownhosts) which associates each host name with its corresponding public key.

Session keys are created when the TOE establishes an SSHv2 connection. The TOE will monitor the time period during which the SSHv2 session keys are active and how much data has been transmitted using them. The TOE has been hard coded to initiate a rekey when the session keys have been used for one hour

(3600 seconds) or when 256 MB of data has been transmitted when TOE acts as a client and 1 GB when the TOE acts as a server. Rekeying is performed upon reaching the threshold that is hit first.

Regardless of whether the TOE is acting as an SSH client or server, all SSHv2 connections will be dropped upon detection of any packet greater than 65535 bytes being transported, as described in RFC 4253. Data encryption is provided by the AES-CBC-128 and AES-CBC-256 encryption algorithms, ecdsa-sha2-nistp256 is used for the public key algorithm, and HMAC-SHA1, HMAC-SHA2-256, and HMAC-SHA2-512 are used for the data integrity algorithms. The key exchange method used in SSHv2 is Diffie-Hellman group 14 with SHA-1.

The SSH public/private key pairs are generated using the following command:

```
ssh server host-key generate
```

The TOE has an "Secure Cryptography Mode" to limit the SSH connection parameters to those defined in the evaluated configuration.

8.2.11 **FCS_TLSC_EXT.1/FCS_TLSS_EXT.1:**

The TOE uses the TLS 1.2 protocol to secure the following connections and channels: web GUI management interface connection using HTTPS (TLS Server), Gigamon Update Server or local Update Server connections using HTTPS (TLS Client) used for TOE image updates, and LDAP server connection (TLS Client) used for authentication requests. When the TOE is operating in "Secure Cryptography Mode", TLS uses the following ciphersuites:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

When the TOE uses TLS client functionality, the presented identifier for the server certificate has to match the reference identifier in order to establish the connection. The hostname reference identifier is the only supported value for the LDAP and update server interface. Regardless of the external interface, wildcards cannot be used when defining the reference identifier on the TOE. The only Supported Elliptic Curves Extension included in the Client Hello is the NIST curve secp256r1. This is not configurable. Certificate pinning is not supported. When certificate validation fails, the connection is not established.

When the TOE uses TLS server functionality, it will reject all connection attempts from TLS versions other than 1.2. EC Diffie-Hellman parameters are generated over NIST curves secp256r1.

8.3 Identification and Authentication

8.3.1 **FIA_AFL.1:**

The TSF provides a configurable counter for consecutive failed authentication attempts that will lock a user account when the failure counter threshold is reached. When an account is locked a user cannot login to either the CLI or web GUI interface. A valid login that happens prior to the failure counter reaching its threshold will reset the counter to zero.

The CLI counter can be set to any 32-bit integer value (a value of 0 will disable lockout). While the user account is locked, no authentication is possible. The authentication failure settings can be configured such

that the default ‘admin’ user account overrides this functionality (exempt) so that it is not possible to cause a denial of service. The lockout duration is a configurable number of seconds, with a default setting of 360.

8.3.2 FIA_PMG_EXT.1:

Passwords maintained by the TSF can be composed using any combination of upper case and lower case letters, numbers, and special characters including the following:
“!”,”@”,”#”,”$”,”%”,”^”,”&”,”*”,”(“,”)”. The password policy is configurable by the Admin and supports the minimum password length of 8 characters and a maximum password length of 30 characters.

8.3.3 FIA_UAU.7:

While authenticating locally to the TOE, the user’s password does not appear in the password field. Instead, asterisks will appear thus masking the password to prevent the password from being shared. In the case that a user enters invalid credentials (valid/invalid username or valid/invalid password), the TOE does not reveal any information about the invalid component of the credential.

8.3.4 FIA_UAU_EXT.2:

Users can authenticate to the TOE locally or remotely. Local users log in to the local console using a username and password via the Serial Port. Remote users can log in to the TOE via the remote CLI using username and password or SSH public key via the Ethernet Management Port. User authentication information that is sent remotely via the remote CLI is protected using SSHv2. Users may also authenticate remotely via a web GUI that is protected using TLS/HTTPS via the Ethernet Management Port. When authenticating using username and password, these credentials are verified using either the TOE's local mechanism and credential repository or by an LDAP server that provides external authentication decisions. For external authentication decisions, the TOE sends an authentication request to the LDAP server which will verify the credentials against the LDAP server's directory and will provide an authentication decision back to the TOE, which is subsequently enforced. The connection between the TOE and the LDAP server is protected by TLS v1.2. When public key authentication is used, the TOE authenticates users by verifying the message the TOE receives from the SSH client using the message's associated public key stored on the TOE.

8.3.5 FIA_UIA_EXT.1:

In the evaluated configuration, the warning banner is displayed prior to the user authenticating to the TOE via the local console, the remote CLI, or the web GUI. The display of the warning banner is the only service that can be run prior to authentication and thus, the TOE does not allow a user to perform any other actions prior to authentication, regardless of the interface used.

8.3.6 FIA_X509_EXT.1/ FIA_X509_EXT.2/ FIA_X509_EXT.3:

The TOE performs certificate validity checking for outbound TLS/HTTPS connections to the Update Server and LDAP Server.

In addition to the validity checking that is performed by the TOE, the TSF will validate certificate revocation status using a certificate revocation list (CRL) that the TSF is configured to download

automatically from a Certification Authority in the Operational Environment. In the event that the revocation status cannot be verified, the certificate will not be accepted.

The TSF determines the validity of certificates by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. In addition, the certificate path is terminated in a trusted CA certificate, the basicConstraints extension is present, and the CA flag is set to TRUE for all CA certificates. The TSF also ensures that the extendedKeyUsage field includes the correct purpose for its intended use. This includes Server Authentication for TLS server certificates; the TSF does not handle TLS client certificates, certificates associated with OCSP responses, or code signing certificates.

In order to support TLS/HTTPS connectivity over the web GUI, the TSF provides the ability to generate a Certificate Request Message as specified by RFC 2986 so that its server certificate can be signed by a Certification Authority. The message includes public key, Common Name, Organization, Organizational Unit, and Country values. The certificate chain of the Certificate Response is validated by the TSF prior to being installed as the TOE's server certificate.

8.4 Security Management

8.4.1 **FMT_MOF.1/ManualUpdate:**

TOE software updates reside on a web server in the Operational Environment. This may be a server maintained by Gigamon or a server within the organization that deploys the TOE. Regardless of where the update resides, it is loaded onto the TOE and applied manually. The Monitor role provides view-only access to ports and configurations. The Admin role is the only administrative role that can perform this action. The TSF restricts the access to this function by enforcing the GigaVUE's role-based access control system.

8.4.2 **FMT_MTD.1/CoreData:**

GigaVUE provides two user roles: Admin and Monitor. The TSF uses role-based access control to assign each user account to one or more roles, each of which has a fixed set of privileges to interact with the product. Of these roles, only the Admin role is authorized to perform the management functions associated with the TSF. The Monitor role provides view-only access to ports and configurations. The Admin role is therefore functionally identical to the 'Security Administrator' as defined by the NDcPP.

The only security-relevant TOE functionality that is available to a user prior to authentication is the display of the warning banner.

8.4.3 **FMT_MTD.1/CryptoKeys:**

The Admin role is the only role that is permitted to manipulate cryptographic data on the TOE. Within the TSF, this behavior is limited to the generation and import/removal of X.509 certificates.

8.4.4 **FMT_SMF.1:**

A user with the Admin role is capable of performing management functions on the TOE locally and remotely. Admins can perform management functions via the local console or remotely via the remote CLI or web GUI. The following table lists the TSF management functions and identifies the interface(s) that can be used to perform them:

Management Function	Local CLI	Remote CLI	Remote GUI
View Audit Data	X	X	
Delete Audit Log	X	X	
Configure TLS Connection Parameters	X	X	X
Configure SSH Connection Parameters	X	X	X
Configure Failed Lockout Threshold	X	X	X
Configure Lockout Duration	X	X	X
Create Users	X	X	X
Modify User Passwords	X	X	X
Modify Password Policy	X	X	X
Configure Supported Authentication Mechanism	X	X	X
Generate X.509 Certificate Request Message	X	X	
Initiate Manual Update	X	X	X
Configure System Time	X	X	X
Configure Idle Session Timeout	X	X	X
Configure Banner Text	X	X	X

Table 8-2: Management Functions by Interface

An Admin can modify the text displayed in the TOE's login banners, set the values for session inactivity before termination, and initiate manual updates to the TOE's software after verifying the digital signature of the update.

The Admin is also able to configure the TOE's cryptographic functionality. This is accomplished by entering a command into the CLI which places the TOE into "Secure Cryptography Mode" of operation. When this command is entered, the TOE limits the cryptographic algorithms to meet the requirements defined within the Security Target.

8.4.5 **FMT_SMR.2:**

The security management functions available to authorized users of the TOE are mediated by a role-based access control system. The role-based access control system is enforced via the local console and remotely via the remote CLI or web GUI. The TOE has two roles: Admin and Monitor. Each role has different authorizations in terms of the functions that they can perform. All SFR relevant management activity is performed by the Admin, role which corresponds to the NDcPP's definition of Security Administrator. Only users with the Admin role are permitted to create and assign roles to users. The Monitor role provides view-only access to ports and configurations.

Each user has the following security attributes associated with them:

- Username
- Password
- SSH public key (optional - used for remote CLI login only)
- One or more roles

The username and password are for authenticating to the TOE. These credentials are verified using the authentication mechanism that has been configured for the TOE. Once the username has been validated, the username is used to query the one or more roles which have been associated with that username

within the TOE's local store. The TOE then uses the roles assigned to the authenticated user to determine if an action is authorized per GigaVUE's role-based access control system. When LDAP authentication is used, that user information is mapped to the internally-stored attributes so that the authentication event is associated with the correct user.

8.5 Protection of the TSF

8.5.1 **FPT_APW_EXT.1:**

The TOE stores usernames and passwords in a password file. All passwords stored on the TOE are stored in hashed form using SHA-512. The password file cannot be viewed by any user on the TOE regardless of the user's role.

8.5.2 **FPT_SKP_EXT.1:**

Public keys are stored in the configuration database which is integrity checked at boot time. Secret/private key data is stored in plaintext on the hard drive but cannot be accessed via the local console, remote CLI, or the web GUI by any user.

8.5.3 **FPT_STM_EXT.1:**

The TOE has an underlying hardware clock that is used for keeping time. A user with the Admin role can set the clock’s time manually. The TSF uses time data for the following purposes:

- Audit record timestamps
- Inactivity timeout for administrative sessions
- Expiration checking for certificates

8.5.4 **FPT_TST_EXT.1:**

All binaries (e.g. executables, libraries), are located on a read-only partition and cannot be modified. In addition, the TOE has a configuration database that is integrity checked at boot time using SHA-1. The udiag is run under u-boot (microcode boot loader) which runs power-on self-tests of all the major components (e.g., memory, CPU, UART, Ethernet controllers) on the motherboard, including the components that connect to the i2c buses. This includes all transceivers used by the data plane. The pci_diag component is a Linux component that runs when the kernel is loading that is responsible for testing and checking the components connected to the PCIe interfaces. It is also responsible for Line card type detection.

Once booted, the TSF will execute a continuous RNG test in order to ensure that the entropy source has not degraded.

If any of the integrity tests fail, diagnostic information is displayed on the boot console indicating what the problem is. For example:

```
POST Failed
Power-up self test failed
cryptographic algorithm test failed.
```

When integrity test fails the TOE is put into safe mode (Gigamon specific state). In safe mode, the device will operate in a limited manner which requires user intervention to bring the appliance back into a normal state after fixing the issues. The console display clearly indicates that the appliance is in safe mode along with the diagnostic information.

These tests are sufficient to validate the correct operation of the TSF because they verify that the cryptographic module is operating correctly, the configuration database does an integrity check, and that the underlying hardware does not have any anomalies that would cause the software to be executed in an unpredictable or inconsistent manner.

8.5.5 **FPT_TUD_EXT.1:**

TOE Admin users can query the current executing version and the most recently installed version of the TOE's firmware/software on the local console, remote CLI interface, and the web GUI interface. On the local console and remote CLI interface a user can enter the "`show version`" command to show both versions of the TOE's firmware/software. Within the web GUI interface, the user can navigate to the "Reboot and Upgrade" tab where both versions of the TOE's firmware/software will be visible.

In order to update the TOE, the Admin can point the TOE directly to the Gigamon Update Server which is a Gigamon hosted site and enter a username and password to download the image. Alternatively, the Admin can download the image themselves and host it on a local server. The Gigamon Update Server is configured to secure the connection using TLS/HTTPS. In the evaluated configuration, any local server used to host the update will also be configured in this manner.

The image that is downloaded is compressed and stored in a tar file and signed with a digital signature. All GigaVUEs are pre-loaded with a key for the signature verification performed as part of the update mechanism. Before the actual installation occurs, the signature is verified against the stored key. The image will not be installed if the update fails to be verified. If the signature is successfully verified, the update will be installed on the inactive partition. If the inactive partition already has a software version installed, the update will over-write the previously installed software. Once the new software is installed, the Admin will enter a command in the local console or remote CLI in order to boot off from the Inactive partition on which the updated was installed, thus making it the active partition.

8.6 TOE Access

8.6.1 **FTA_SSL_EXT.1:**

The TOE is designed to terminate a local session after a specific period of time. The default setting is 15 minutes and it is configurable by an Admin. Once a session has been terminated, the local user must re-authenticate to start a new session.

8.6.2 **FTA_SSL.3:**

The TOE can be configured to terminate remote interactive sessions that are inactive in two different ways. In the event that the inactivity setting is met while users are logged into the CLI, the TOE tears down the SSH connection. This setting can be configured to 0 or between .25-35791 minutes. The value of 0 means that this setting is disabled and there is no timeout configured. In the event that the inactivity setting is reached while a user is logged into the web GUI, the user's session will end. This setting can be

configured between 0-525600 minutes. The value of 0 means that this setting is disabled and there is no timeout configured.

The Admin users authenticated to the local console or remote CLI may configure this setting for all of the local console, remote CLI, and web GUI. However, Admin users authenticated to the web GUI can only configure the timeout setting for the web GUI.

8.6.3 **FTA_SSL.4:**

An Admin is able to terminate their own session by entering the "exit" command when logged into the local console or remote CLI. An Admin can terminate their own session by clicking on the "Logout" tab when logged into the web GUI.

8.6.4 **FTA_TAB.1:**

There are three possible ways to authenticate to the TOE: local console, remote CLI, and web GUI. Each of these interfaces has a configurable login banner that is displayed prior to the user authenticating to the TOE.

The banner is configured using the “banner login-local” command for the local console and “banner login-remote” for both the remote CLI and web GUI. The command “banner login” configures the banner for all login methods.

8.7 Trusted Path/Channels

8.7.1 **FTP_ITC.1:**

The TOE connects and sends data to IT entities that reside in the Operational Environment via trusted channels. In the evaluated configuration, the TOE connects with a Syslog Server using SSHv2 to encrypt the audit data that traverses the channel. When remote authentication is configured, the TOE connects to an LDAP Server using TLS v1.2 to send authentication requests for a user attempting to login to the local console, remote CLI, or web GUI. The TOE can also connect to the Gigamon Update Server or a local Update Server using TLS/HTTPS (TLS v1.2) to download TOE software updates. The remote endpoints are authenticated using TLS server certificates and SSH host keys.

In each of these instances, the TOE initiates communication as the client using the cryptographic protocol in the manner described by their respective SFRs. These protocols are used to protect the data traversing the channel from disclosure and/or modification.

8.7.2 **FTP_TRP.1/Admin:**

The Admin users are required to authenticate to the TOE in order to be able to perform any management functions. By initiating the trusted path via the web GUI or remote CLI, Admin users can perform management activities remotely. The web GUI path is protected by TLS/HTTPS (TLS v1.2) and the remote CLI is protected using SSHv2. These protocols are used to protect the data traversing the channel from disclosure and/or modification.

9 Appendix A: Audit Event Samples

Auditable Event	Sample Data
Start-up and shut-down of the audit functions	**Startup of audit functions** Aug 16 11:26:27 gigamonTA100 mgmtd[898]: [mgmtd.INFO]: Config change ID 2: requested by: user admin (System Administrator) via CLI, 1 item(s) changed Aug 16 11:26:27 gigamonTA100 mgmtd[898]: [mgmtd.INFO]: Config change ID 2: item 1: syslog: local file sink /var/log/messages: minimum log severity changed from "none" to "info" **Shutdown of audit functions** Aug 16 11:26:05 gigamonTA100 cli[11597]: [cli.INFO]: user admin: Executing command: logging local none
Administrative login and logout	**Local Console login using password** Mar 28 07:21:56 gigamonTA100 login: pam_unix(login:session): session opened for user admin by LOGIN(uid=0) Mar 28 07:21:56 gigamonTA100 login: DIALUP AT ttyS0 BY admin Mar 28 07:21:56 gigamonTA100 login: ROOT LOGIN ON ttyS0: user admin (System Administrator) Mar 28 07:21:56 gigamonTA100 cli[26148]: [cli.NOTICE]: user admin: CLI module launched Mar 28 07:21:56 gigamonTA100 mgmtd[1105]: [mgmtd.NOTICE]: User admin (local user admin) authentication method: local **CLI Logout:** Feb 16 11:01:22 gigamonTA10 cli[18175]: [cli.INFO]: user admin: Executing command: exit Feb 16 11:01:22 gigamonTA10 cli[18175]: [cli.INFO]: user admin: session 1: closing for peer mgmtd user i:2223-0-0 (0/0) 0 Feb 16 11:01:22 gigamonTA10 mgmtd[2223]: [mgmtd.INFO]: session 46: closing for peer cli-18175 user admin (0/0) 1 Feb 16 11:01:22 gigamonTA10 cli[18175]: [cli.INFO]: user admin: libevent: escaping from dispatch (sticky) Feb 16 11:01:22 gigamonTA10 mgmtd[2223]: [mgmtd.INFO]: EVENT: /mgmtd/session/events/logout Feb 16 11:01:22 gigamonTA10 mgmtd[2223]: [mgmtd.INFO]: Calling internal interest callback for event /mgmtd/session/events/logout Feb 16 11:01:22 gigamonTA10 mgmtd[2223]: [mgmtd.INFO]: Calling internal interest callback for event /mgmtd/session/events/logout

	Feb 16 11:01:22 gigamonTA10 mgmtd[2223]: [mgmtd.NOTICE]: User admin: logout from 192.168.1.3 through trusted cli channel. Feb 16 11:01:22 gigamonTA10 cli[18175]: [cli.INFO]: user admin: session 1: closing, but already closed Feb 16 11:01:22 gigamonTA10 cli[18175]: [cli.NOTICE]: user admin: CLI exiting Feb 16 11:01:22 gigamonTA10 sshd[18172]: [INFO]: Received disconnect from 192.168.1.3: 11: disconnected by user Feb 16 11:01:22 gigamonTA10 sshd[18172]: pam_unix(sshd:session): session closed for user admin **Remote GUI login using password** Mar 28 06:20:58 gigamonTA100 wsmd[1239]: [wsmd.INFO]: session 1: client open for peer mgmtd (local name wsmd.3-1239) Mar 28 06:20:58 gigamonTA100 wsmd[1239]: [wsmd.NOTICE]: User admin (System Administrator) logged into Web UI from 192.168.1.25 Mar 28 06:20:58 gigamonTA100 ugwd[1251]: [ugwd.INFO]: remote user id: admin, local user id: admin Mar 28 06:20:58 gigamonTA100 mgmtd[1105]: [mgmtd.NOTICE]: User admin (local user admin) authentication method: local **Remote GUI logout** Feb 16 11:10:00 gigamonTA10 wsmd[2323]: [wsmd.NOTICE]: User admin from 192.168.1.98 logged out of Web UI Feb 16 11:10:00 gigamonTA10 wsmd[2323]: [wsmd.INFO]: session 1: closing for peer mgmtd user i:2223-0-0 (0/0) 0 Feb 16 11:10:00 gigamonTA10 wsmd[2323]: [wsmd.INFO]: Web session 2 closed Feb 16 11:10:00 gigamonTA10 wsmd[2323]: [wsmd.INFO]: Recording web logout of user admin on device /dev/web/2 **Local Console login and logout using LDAP password** May 3 07:58:33 gigamonTA100 login: pam_ldap: connection established to LDAP testUser1@server ldap.catl.local:636: May 3 07:58:33 gigamonTA100 login: pam_unix(login:session): session opened for user testUser1 (admin) by LOGIN(uid=0) May 3 07:58:33 gigamonTA100 login: DIALUP AT ttyS0 BY admin May 3 07:58:33 gigamonTA100 login: ROOT LOGIN ON ttyS0: user admin (System Administrator) May 3 07:58:33 gigamonTA100 cli[926]: [cli.NOTICE]: user testUser1 (local user admin): CLI module launched

	May 3 07:58:33 gigamonTA100 login: pam_ldap: connection closed to LDAP admin@server ldap.catl.local:636: **Remote GUI login and logout using LDAP password** Mar 28 06:30:39 gigamonTA100 wsmd[1239]: pam_ldap: connection established to LDAP testUser1@server ldap.catl.local:636: Mar 28 06:30:39 gigamonTA100 wsmd[1239]: [wsmd.INFO]: Web session 4 created Mar 28 06:30:39 gigamonTA100 wsmd[1239]: [wsmd.INFO]: Recording web login of user admin on device /dev/web/4 Mar 28 06:30:39 gigamonTA100 mgmtd[1105]: [mgmtd.INFO]: Opened session: 59 Mar 28 06:30:39 gigamonTA100 mgmtd[1105]: [mgmtd.INFO]: session 59: opened for client wsmd.4-1239 user testUser1 (0/0) 1 Mar 28 06:30:39 gigamonTA100 mgmtd[1105]: [mgmtd.NOTICE]: User testUser1 (local user admin) authentication method: ldap Mar 28 06:30:39 gigamonTA100 wsmd[1239]: pam_ldap: connection closed to LDAP admin@server ldap.catl.local:636: **Remote SSH login and logout using LDAP password** Mar 28 06:43:34 gigamonTA100 sshd[23511]: pam_ldap: connection established to LDAP testUser1@server ldap.catl.local:636: Mar 28 06:43:34 gigamonTA100 sshd[23509]: [NOTICE]: User admin (System Administrator) logged in via ssh2 from 192.168.1.25 port 51312 Mar 28 06:43:34 gigamonTA100 sshd[23509]: pam_unix(sshd:session): session opened for user testUser1 (admin) by (uid=0) Mar 28 06:43:34 gigamonTA100 sshd[23509]: [INFO]: subsystem request for sftp by user admin Mar 28 06:43:34 gigamonTA100 cli[23513]: [cli.NOTICE]: user testUser1 (local user admin): CLI module launched Mar 28 06:43:34 gigamonTA100 sshd[23511]: pam_ldap: connection closed to LDAP admin@server ldap.catl.local:636: **Remote SSH login using public key** May 1 08:21:14 gigamonTA100 sshd[21781]: [INFO (verbose)]: Set /proc/self/oom_score_adj to 0 May 1 08:21:14 gigamonTA100 sshd[21781]: [INFO (verbose)]: Connection from 192.168.1.98 port 4597 May 1 08:21:15 gigamonTA100 sshd[21781]: [INFO (verbose)]: Found matching RSA key: 79:96:a1:17:48:ba:a0:ba:8f:55:24:58:f8:e3:ed:2d:a2:91:d1:90 [SHA-1]

	May 1 08:21:15 gigamonTA100 sshd[21781]: [INFO (verbose)]: Postponed publickey for admin from 192.168.1.98 port 4597 ssh2 [preauth] May 1 08:21:17 gigamonTA100 sshd[21781]: [INFO (verbose)]: Found matching RSA key: 79:96:a1:17:48:ba:a0:ba:8f:55:24:58:f8:e3:ed:2d:a2:91:d1:90 [SHA-1] May 1 08:21:17 gigamonTA100 sshd[21781]: [INFO]: Accepted publickey for admin from 192.168.1.98 port 4597 ssh2 May 1 08:21:17 gigamonTA100 sshd[21781]: [NOTICE]: User admin (System Administrator) logged in via ssh2 from 192.168.1.98 port 4597 **Remote SSH login using password** Mar 28 05:05:29 gigamonTA100 sshd[16580]: [NOTICE]: User admin (System Administrator) logged in via ssh2 from 192.168.1.25 port 64642 Mar 28 05:05:29 gigamonTA100 sshd[16580]: pam_unix(sshd:session): session opened for user admin by (uid=0) Mar 28 05:05:29 gigamonTA100 sshd[16580]: [INFO]: subsystem request for sftp by user admin Mar 28 05:05:29 gigamonTA100 cli[16584]: [cli.NOTICE]: user admin: CLI module launched
Unsuccessful login attempts limit is met or exceeded.	**(CLI) Unsuccessful login attempts** Jul 11 11:52:16 gigamonTA100 sshd[27189]: [ERR]: User admin (System Administrator) failed to login via ssh2 from 192.168.1.152 port 50994 Jul 11 11:52:24 gigamonTA100 sshd[27189]: [ERR]: User admin (System Administrator) failed to login via ssh2 from 192.168.1.152 port 50994 Jul 11 11:52:46 gigamonTA100 sshd[27189]: [ERR]: User admin (System Administrator) failed to login via ssh2 from 192.168.1.152 port 50994 Jul 11 11:53:02 gigamonTA100 sshd[27285]: [ERR]: User admin (System Administrator) failed to login via ssh2 from 192.168.1.152 port 50996 Jul 11 11:53:14 gigamonTA100 sshd[27285]: [ERR]: User admin (System Administrator) failed to login via ssh2 from 192.168.1.152 port 50996 Jul 11 11:53:14 gigamonTA100 sshd[27303]: pam_tallybyname(sshd:auth): Denying access to user 'admin': Maximum number of failed logins reached, account locked. You may try again in 57 second(s). **(GUI) Unsuccessful login attempts** Jul 20 13:28:11 gigamonTA100 wsmd[1271]: [wsmd.NOTICE]: Authentication failure for user admin from 192.168.1.98 Jul 20 13:28:22 gigamonTA100 wsmd[1271]: [wsmd.NOTICE]: Authentication failure for user admin from 192.168.1.98

	Jul 20 13:28:28 gigamonTA100 wsmd[1271]: [wsmd.NOTICE]: Authentication failure for user admin from 192.168.1.98 Jul 20 13:28:34 gigamonTA100 wsmd[1271]: [wsmd.NOTICE]: Authentication failure for user admin from 192.168.1.98 Jul 20 13:28:40 gigamonTA100 wsmd[1271]: [wsmd.NOTICE]: Authentication failure for user admin from 192.168.1.98 Jul 20 13:28:49 gigamonTA100 wsmd[1271]: pam_tallybyname(wsmd:auth): Denying access to user 'admin': Maximum number of failed logins reached, account locked. You may try again in 46 second(s).
Security related configuration changes	**(CLI) Administrator configured login banner** Mar 28 01:19:21 gigamonTA100 cli[938]: [cli.INFO]: user admin: Check admin default password Mar 28 01:19:21 gigamonTA100 cli[938]: [cli.INFO]: user admin: CLI initialized, entering main event loop Mar 28 01:19:33 gigamonTA100 cli[938]: [cli.INFO]: user admin: Executing command: enable Mar 28 01:19:33 gigamonTA100 cli[938]: [cli.NOTICE]: user admin: Entering enable mode Mar 28 01:19:36 gigamonTA100 cli[938]: [cli.INFO]: user admin: Executing command: config t Mar 28 01:19:36 gigamonTA100 cli[938]: [cli.NOTICE]: user admin: Entering configuration mode Mar 28 01:19:39 gigamonTA100 ugwd[1251]: [ugwd.INFO]: remote_chassis_msg_report standalone sends no report Mar 28 01:20:00 gigamonTA100 cli[938]: [cli.INFO]: user admin: Executing command: banner login "!!THIS IS A WARNING BANNER!!" **(GUI) Administrator configured login banner** Mar 28 02:49:21 gigamonTA100 mgmtd[1105]: [mgmtd.INFO]: Calling apply function for module changes:-10000:0 Mar 28 02:49:21 gigamonTA100 mgmtd[1105]: [mgmtd.INFO]: Config change ID 26: requested by: user admin (System Administrator) via ugwc.0-1251, 1 item(s) changed Mar 28 02:49:21 gigamonTA100 mgmtd[1105]: [mgmtd.INFO]: Config change ID 26: item 1: login message: network ("issue_net") changed from "!!THIS IS A WARNING BANNER!!" to "!@THIS IS A WARNING BANNER@!" Mar 28 02:49:21 gigamonTA100 mgmtd[1105]: [mgmtd.INFO]: EVENT: /mgmtd/notify/dbchange/as_saved

Generating/import of, changing, or deleting of cryptographic keys	**Generation of SSH host keys** Nov 27 14:34:37 gigamonTA100 cli[2865]: [cli.INFO]: user admin: Executing command: ssh server host-key generate Nov 27 14:34:37 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 152: requested by: user admin (System Administrator) via CLI Nov 27 14:34:37 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 152: descr: regenerate SSH host keys
Resetting passwords	**(CLI) Successful password change for user cctl to aA67890#$%^&*()** Nov 20 11:11:42 gigamonTA100 cli[15840]: [cli.INFO]: user admin: Executing command matching: username cctl password * Nov 20 11:11:42 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 34: param: username: "cctl" Nov 20 11:11:42 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: SET: /auth/passwd/user/cctl/password Nov 20 11:11:42 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: SET: /auth/passwd/user/cctl/enable Nov 20 11:11:42 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Successfully updated user cctl Nov 20 11:11:42 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Config change ID 63: item 1: local user account 'cctl': password changed from (undisclosed password set) to (undisclosed password set) **(CLI) Successful login for user cctl using password aA67890#$%^&*()** Nov 20 11:12:22 gigamonTA100 sshd[17212]: [NOTICE]: User cctl logged in via ssh2 from 192.168.1.225 port 56066 Nov 20 11:12:22 gigamonTA100 sshd[17212]: pam_unix(sshd:session): session opened for user cctl by (uid=0) Nov 20 11:12:22 gigamonTA100 cli[17219]: [cli.NOTICE]: user cctl: CLI module launched Nov 20 11:12:22 gigamonTA100 cli[17219]: [cli.INFO]: user cctl: session 1: client open for peer mgmtd (local name cli-17219) Nov 20 11:12:22 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: session 162: opened for client cli-17219 user cctl (0/0) 1 Nov 20 11:12:22 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: TRUSTED_AUTH_INFO (user cctl/cctl): validated OK Nov 20 11:12:22 gigamonTA100 mgmtd[835]: [mgmtd.NOTICE]: User cctl (local user cctl) authentication method: local

	Nov 20 11:12:22 gigamonTA100 mgmtd[835]: [mgmtd.NOTICE]: User cctl: login from 192.168.1.225 through trusted cli channel. **(GUI) Successful password change for user cctl to aA67890#$%^&*()** Nov 20 12:02:01 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 45: param: username: "cctl" Nov 20 12:02:01 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: SET: /auth/passwd/user/cctl/password Nov 20 12:02:01 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: SET: /auth/passwd/user/cctl/enable Nov 20 12:02:01 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Successfully updated user cctl Nov 20 12:02:01 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Config change ID 70: item 1: local user account 'cctl': password changed from (undisclosed password set) to (undisclosed password set) **(GUI) Successful log in for user cctl with password aA67890#$%^&*()** Nov 20 12:02:19 gigamonTA100 wsmd[942]: [wsmd.INFO]: Recording web login of user cctl on device /dev/web/28 Nov 20 12:02:19 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: session 185: opened for client wsmd.28-942 user cctl (0/0) 1 Nov 20 12:02:19 gigamonTA100 wsmd[942]: [wsmd.NOTICE]: User cctl logged into Web UI from 192.168.1.225 Nov 20 12:02:19 gigamonTA100 ugwd[948]: [ugwd.INFO]: remote user id: cctl, local user id: cctl Nov 20 12:02:19 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: TRUSTED_AUTH_INFO (user cctl/cctl): validated OK
Failure to establish an HTTPS session	**Failure to establish session (HTTPS):** Jul 5 13:38:25 gigamonTA100 httpd[26802]: [Thu Jul 05 13:38:25 2018] [error] [client 192.168.1.98] SSL library error 1 in handshake (server gigamonTA100:443) Jul 5 13:38:25 gigamonTA100 httpd[26802]: [Thu Jul 05 13:38:25 2018] [error] SSL Library Error: 336109761 error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher Too restrictive SSLCipherSuite or using DSA server certificate? **Session establishment (HTTPS):** Jul 5 13:36:43 gigamonTA100 wsmd[1328]: [wsmd.INFO]: Web session 2 created Jul 5 13:36:43 gigamonTA100 mgmtd[1147]: [mgmtd.NOTICE]: User admin: login from 192.168.1.98 through trusted web channel. Jul 5 13:36:43 gigamonTA100 wsmd[1328]: [wsmd.NOTICE]: User admin (System Administrator) logged into Web UI from 192.168.1.98

	Session termination (HTTPS): Jul 5 13:37:33 gigamonTA100 wsmd[1328]: [wsmd.NOTICE]: User admin from 192.168.1.98 logged out of Web UI Jul 5 13:37:33 gigamonTA100 wsmd[1328]: [wsmd.INFO]: session 1: closing for peer mgmtd user i:1147-0-0 (0/0) 0 Jul 5 13:37:33 gigamonTA100 wsmd[1328]: [wsmd.INFO]: Web session 2 closed
Failure to establish an SSH session	**Failure to establish SSH session**: Nov 15 09:34:55 gigamonTA100 sshd[22373]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.225 user=admin Nov 15 09:35:00 gigamonTA100 sshd[22371]: [ERR]: PAM: Authentication failure for admin from 192.168.1.225 Nov 15 09:35:00 gigamonTA100 sshd[22371]: [ERR]: User admin (System Administrator) failed to login via ssh2 from 192.168.1.225 port 53615 **Session establishment (SSH)**: Nov 15 09:29:31 gigamonTA100 sshd[22027]: [INFO (verbose)]: Connection from 192.168.1.225 port 53463 Nov 15 09:29:37 gigamonTA100 sshd[22027]: [NOTICE]: User admin (System Administrator) logged in via ssh2 from 192.168.1.225 port 53463 **Session termination (SSH):** Nov 24 14:59:43 gigamonTA100 sshd[2049]: pam_unix(sshd:session): session closed for user admin
Failure to establish a TLS session	**Failure to establish session (TLS):** Jul 12 09:40:31 gigamonTA100 mgmtd[1147]: [mgmtd.NOTICE]: Exit with code 35 from curl: error:1409210A:SSL routines:ssl3_get_server_hello:wrong ssl version Jul 12 09:40:31 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: Download of /var/opt/tms/images/.temp/catlsvcs.catl.local complete, now 0 downloads active Jul 12 09:40:31 gigamonTA100 mgmtd[1147]: [mgmtd.ERR]: Set commit return status: code 0x1, message: error:1409210A:SSL routines:ssl3_get_server_hello:wrong ssl version Jul 12 09:40:31 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: Action ID 134: status: completed with failure **Session establishment (TLS):** Jul 12 09:40:25 gigamonTA100 cli[20427]: [cli.INFO]: user admin: Executing command: image fetch https://catlsvcs.catl.local Jul 12 09:40:25 gigamonTA100 cli[20427]: [cli.INFO]: user admin: Tracking progress on operation ID cli-20427-105 Jul 12 09:40:25 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: Action ID 134: requested by: user admin (System Administrator) via CLI Jul 12 09:40:25 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: Opened session: 169 ul 12 09:40:25 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: session 169: opened for client progress-20814 user i:20814-0-0 (0/0) 0 **Session termination (TLS):**

	Jul 12 09:40:31 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: session 169: closing for peer progress-20814 user i:20814-0-0 (0/0) 0
All use of the identification and authentication mechanism	See 'Administrative login and logout'
Unsuccessful attempt to validate a certificate	**Issuer Certificate Failed** Jul 11 14:10:02 gigamonTA100 mgmtd[1147]: [mgmtd.NOTICE]: Exit with code 60 from curl: CAfile: /etc/pki/tls/certs/ca-bundle.crt CApath: /var/opt/tms/output/cacerts } [5 bytes data] } [183 bytes data] { [94 bytes data] { [2821 bytes data] } [2 bytes data] } [5 bytes data] } [2 bytes data] curl: (60) SSL certificate problem: unable to get issuer certificate More details here: https://curl.haxx.se/docs/sslcerts.html curl failed to verify the legitimacy of the server and therefore could not establish a secure connection to it. To learn more about this situation and how to fix it, please visit the web page mentioned above. **Certificate Expired** Jul 11 14:28:02 gigamonTA100 mgmtd[1147]: [mgmtd.NOTICE]: Exit with code 60 from curl: CAfile: /etc/pki/tls/certs/ca-bundle.crt CApath: /var/opt/tms/output/cacerts } [5 bytes data] } [183 bytes data] { [94 bytes data] { [5972 bytes data] } [2 bytes data] } [5 bytes data] } [2 bytes data] curl: (60) SSL certificate problem: certificate has expired More details here: https://curl.haxx.se/docs/sslcerts.html curl failed to verify the legitimacy of the server and therefore could not establish a secure connection to it. To learn more about this situation and how to fix it, please visit the web page mentioned above. **Certificate Revoked** Jul 27 10:50:10 gigamonTA100 mgmtd[1131]: [mgmtd.NOTICE]: Exit with code 60 from curl: CAfile: /etc/pki/tls/certs/ca-bundle.crt CApath: /var/opt/tms/output/cacerts } [5 bytes data] } [159 bytes data] { [94 bytes data] { [5972 bytes data] } [2 bytes data] } [5 bytes data] } [2 bytes data] curl: (60) SSL certificate problem: certificate revoked More details here: https://curl.haxx.se/docs/sslcerts.html curl failed to verify the legitimacy of the server and therefore could not establish a secure connection to it. To learn more about this situation and how to fix it, please visit the web page mentioned above. **Peer Certificate Revoked** Jul 27 13:27:09 gigamonTA100 mgmtd[1131]: [mgmtd.NOTICE]: Exit with code 60 from curl: CAfile: /etc/pki/tls/certs/ca-bundle.crt CApath: /var/opt/tms/output/cacerts } [5 bytes data] } [159 bytes data] { [94 bytes data] { [5972 bytes data] } [2 bytes data] } [5 bytes data] } [2 bytes data] curl: (60) SSL certificate problem: certificate revoked More details here: https://curl.haxx.se/docs/sslcerts.html curl failed to verify the legitimacy of the

	server and therefore could not establish a secure connection to it. To learn more about this situation and how to fix it, please visit the web page mentioned above. **Peer Certificate not authenticated** Dec 14 17:28:35 gigamonTA100 mgmtd[874]: [mgmtd.NOTICE]: Exit with code 60 from curl: CApath: /var/opt/tms/output/cacerts curl: (60) Peer certificate cannot be authenticated with known CA certificates More details here: http://curl.haxx.se/docs/sslcerts.html curl performs SSL certificate verification by default, using a "bundle" of Certificate Authority (CA) public keys (CA certs). If the default bundle file isn't adequate, you can specify an alternate file using the --cacert option. If this HTTPS server uses a certificate signed by a CA represented in the bundle, the certificate verification probably failed due to a problem with the certificate (it might be expired, or the name might not match the domain name in the URL). If you'd like to turn off curl's verification of the certificate, use the -k (or --insecure) option. Dec 14 17:28:35 gigamonTA100 mgmtd[874]: [mgmtd.INFO]: Download of /var/opt/tms/images/.temp/catlsvcs.cctl.com complete, now 0 downloads active Dec 14 17:28:35 gigamonTA100 mgmtd[874]: [mgmtd.ERR]: Set commit return status: code 0x1, message: SSL certificate verification failed. **Missing CRL Signing** Aug 6 13:54:49 gigamonTA100 sshd[15226]: pam_ldap: ldap_simple_bind: server genericopenssl.catl.local:636: Can't contact LDAP server: certificate verify failed (key usage does not include CRL signing) Aug 6 14:18:59 gigamonTA100 mgmtd[1130]: [mgmtd.NOTICE]: Exit with code 60 from curl: CAfile: /etc/pki/tls/certs/ca-bundle.crt CApath: /var/opt/tms/output/cacerts } [5 bytes data] } [165 bytes data] { [94 bytes data] { [4990 bytes data] } [2 bytes data] } [5 bytes data] } [2 bytes data] curl: (60) SSL certificate problem: key usage does not include CRL signing More details here: https://curl.haxx.se/docs/sslcerts.html curl failed to verify the legitimacy of the server and therefore could not establish a secure connection to it. To learn more about this situation and how to fix it, please visit the web page mentioned above. **Invalid CA** Jul 12 08:20:34 gigamonTA100 mgmtd[1147]: [mgmtd.NOTICE]: Exit with code 60 from curl: CAfile: /etc/pki/tls/certs/ca-bundle.crt CApath: /var/opt/tms/output/cacerts } [5 bytes data] } [189 bytes data] { [94 b ytes data] { [784 bytes data] } [2 bytes data] } [5 bytes data] } [2 bytes data] curl: (60) SSL certificate problem: invalid CA certificate More details here: https://curl.haxx.se/docs/sslcerts.html curl failed

	to verify the legitimacy of the server and therefore could not establish a secure connection to it. To learn more about this situation and how to fix it, please visit the web page mentioned above.
Any attempt to initiate a manual update	See 'Initiation of update; result of the update attempt'
All management activities of TSF data	See 'Security related configuration changes'
Changes to the time	**(Remote CLI) Changes to Date & Time** Nov 20 15:16:29 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 75: descr: system clock: set date and time Nov 20 15:16:29 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 75: param: date and time: 2017/12/20 10:00:00 Dec 20 10:00:00 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: EVENT: /time/notify/time_change Dec 20 10:00:00 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Calling internal interest callback for event /time/notify/time_change Dec 20 10:00:00 gigamonTA100 sched[946]: [sched.INFO]: Processing event: /time/notify/time_change **(GUI) Changes to Date & Time** Nov 20 15:23:06 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: SET: /time/zone Nov 20 15:23:06 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 77: descr: system clock: set date and time Nov 20 15:23:06 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 77: param: date and time: 2017/12/20 10:00:00 Dec 20 10:00:01 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: EVENT: /time/notify/time_change Dec 20 10:00:01 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Calling internal interest callback for event /time/notify/time_change Dec 20 10:00:01 gigamonTA100 sched[946]: [sched.INFO]: Processing event: /time/notify/time_change **(Local CLI) Changes to Time** Nov 29 10:00:13 gigamonTA100 cli[22684]: [cli.INFO]: user admin: Executing command: clock set 09:21:00 2017/11/29 Nov 29 10:00:13 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 198: requested by: user admin (System Administrator) via CLI Nov 29 10:00:13 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 198: descr: system clock: set date and time Nov 29 10:00:13 gigamonTA100 mgmtd[835]: [mgmtd.INFO]: Action ID 198:

	param: date and time: 2017/11/29 09:21:00
Initiation of update; result of the update attempt	**Initiation of update (CLI)** Aug 1 11:42:23 gigamonTA100 cli[1521]: [cli.INFO]: user admin: Executing command: image install ta100_510103.img Aug 1 11:42:23 gigamonTA100 cli[1521]: [cli.INFO]: user admin: Tracking progress on operation ID cli-1521-223 Aug 1 11:42:23 gigamonTA100 mgmtd[1131]: [mgmtd.INFO]: Action ID 5: requested by: user admin (System Administrator) via CLI Aug 1 11:42:23 gigamonTA100 mgmtd[1131]: [mgmtd.INFO]: Action ID 5: descr: install system software image Aug 1 11:42:23 gigamonTA100 mgmtd[1131]: [mgmtd.INFO]: Action ID 5: param: image filename: ta100_510103.img, version: GigaVUE-OS 5.1.01.03 Build 98285 2018-07-22 11:10:02 x86_64 gitac root@jenkins-slave318:git:73d6a8353a7b Aug 1 11:42:23 gigamonTA100 mgmtd[1131]: [mgmtd.INFO]: Action ID 5: param: switch next boot location after install: no Aug 1 11:42:23 gigamonTA100 mgmtd[1131]: [mgmtd.INFO]: Tracking image install progress under operation ID cli-1521-223 Aug 1 11:42:23 gigamonTA100 mgmtd[1131]: [mgmtd.NOTICE]: Installing verified image: /var/opt/tms/images/ta100_510103.img Aug 1 11:43:39 gigamonTA100 mgmtd[1131]: [mgmtd.NOTICE]: Image installation finished successfully **Initiation of update (GUI)** Aug 1 12:17:09 gigamonTA100 mgmtd[1130]: [mgmtd.INFO]: Action ID 3: requested by: user admin (System Administrator) via ugwc.0-1282 Aug 1 12:17:09 gigamonTA100 mgmtd[1130]: [mgmtd.INFO]: Action ID 3: descr: install system software image Aug 1 12:17:09 gigamonTA100 mgmtd[1130]: [mgmtd.INFO]: Action ID 3: param: image filename: ta100_510103.img, version: GigaVUE-OS 5.1.01.03 Build 98285 2018-07-22 11:10:02 x86_64 gitac root@jenkins-slave318:git:73d6a8353a7b Aug 1 12:17:09 gigamonTA100 mgmtd[1130]: [mgmtd.INFO]: Action ID 3: param: target boot location ID: 2 Aug 1 12:17:09 gigamonTA100 mgmtd[1130]: [mgmtd.INFO]: Action ID 3: param: switch next boot location after install: yes Aug 1 12:17:09 gigamonTA100 mgmtd[1130]: [mgmtd.NOTICE]: Installing verified image: /var/opt/tms/images/ta100_510103.img Aug 1 12:18:28 gigamonTA100 mgmtd[1130]: [mgmtd.NOTICE]: Image installation finished successfully

Any attempts of unlocking of an interactive session	**Session termination due to inactivity (local console)** Nov 21 14:49:36 gigamonTA100 mgmtd[835]: [mgmtd.NOTICE]: User admin: login from 192.168.1.225 through trusted cli channel. Nov 21 14:53:37 gigamonTA100 cli[17689]: [cli.NOTICE]: user admin: Inactive for 4 minutes -- automatically logging out
The termination of a remote session by the session locking mechanism	**Session termination due to inactivity (GUI):** Jul 20 12:06:55 gigamonTA100 wsmd[1271]: [wsmd.NOTICE]: User admin (System Administrator) logged into Web UI from 192.168.1.98 Jul 20 12:10:56 gigamonTA100 wsmd[1271]: [wsmd.NOTICE]: Web session 3 is closed by timeout, idle time: 240
The termination of an interactive session	**Manual session termination by admin (CLI)** Nov 21 16:38:47 gigamonTA100 mgmtd[835]: [mgmtd.NOTICE]: User admin: logout from 192.168.1.225 through trusted cli channel. Nov 21 16:38:50 gigamonTA100 sshd[25723]: [INFO]: Received disconnect from 192.168.1.225: 11: FlowSshClientSession: disconnected on user's request **Manual session termination by admin (Web GUI)** Nov 21 16:49:40 gigamonTA100 mgmtd[835]: [mgmtd.NOTICE]: User admin: logout from 192.168.1.225 through trusted web channel.
Initiation of the trusted channel	**Initiation of the trusted channel (HTTPS update web server)** Aug 7 12:13:36 gigamonTA100 cli[21264]: [cli.INFO]: user admin: Executing command: image fetch https://catlsvcs.catl.local Aug 7 12:13:36 gigamonTA100 cli[21264]: [cli.INFO]: user admin: Tracking progress on operation ID cli-21264-74 Aug 7 12:13:36 gigamonTA100 mgmtd[1130]: [mgmtd.INFO]: Action ID 12: requested by: user admin (System Administrator) via CLI Aug 7 12:13:36 gigamonTA100 mgmtd[1130]: [mgmtd.INFO]: Beginning download of /var/opt/tms/images/.temp/catlsvcs.catl.local, now 1 downloads active Aug 7 12:13:36 gigamonTA100 progress[22403]: [progress.INFO]: Process with pid 22404: launched (not waiting for it) Aug 7 12:13:36 gigamonTA100 progress[22403]: [progress.INFO]: Progress: got total file size from HTTP header: 1138 bytes. Aug 7 12:13:36 gigamonTA100 progress[22403]: [progress.INFO]: Received signal SIGCHLD **Initiation of the trusted channel (Remote syslog via SSH)** Aug 7 12:07:45 gigamonTA100 mgmtd[21783]: [mgmtd.NOTICE]: SSH connection to cctl@192.168.1.152:514 established

	Initiation of the trusted channel (LDAP authentication server) Aug 7 11:50:05 gigamonTA100 sshd[19825]: pam_ldap: connection established to LDAP testUser1@server ldap.catl.local:636:
Termination of the trusted channel	**Termination of the trusted channel (HTTPS update web server)** Aug 7 12:13:36 gigamonTA100 progress[22403]: [progress.INFO]: session 1: closing for peer mgmtd user i:1130-0-0 (0/0) 0 Aug 7 12:13:36 gigamonTA100 progress[22403]: [progress.INFO]: libevent: escaping from dispatch (sticky) Aug 7 12:13:36 gigamonTA100 progress[22403]: [progress.INFO]: session 1: closing, but already closed Aug 7 12:13:36 gigamonTA100 mgmtd[1130]: [mgmtd.INFO]: Download of /var/opt/tms/images/.temp/catlsvcs.catl.local complete, now 0 downloads active Aug 7 12:13:36 gigamonTA100 mgmtd[1130]: [mgmtd.INFO]: Action ID 12: status: completed with success **Termination of the trusted channel (Remote syslog via SSH)** Aug 7 12:07:50 gigamonTA100 mgmtd[1130]: [mgmtd.NOTICE]: SSH connections to all remote syslog servers are being closed and restarted **Termination of the trusted channel (LDAP authentication server)** Aug 7 11:50:05 gigamonTA100 sshd[19825]: pam_ldap: connection closed to LDAP admin@server ldap.catl.local:636:
Failure of the trusted channel functions	**Failure of the trusted channel functions (HTTPS update web server)** Aug 7 12:16:31 gigamonTA100 cli[21264]: [cli.INFO]: user admin: Executing command: image fetch https://catlsvcs.catl.local Aug 7 12:16:31 gigamonTA100 mgmtd[1130]: [mgmtd.NOTICE]: Exit with code 35 from curl: error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure Aug 7 12:16:31 gigamonTA100 mgmtd[1130]: [mgmtd.INFO]: Download of /var/opt/tms/images/.temp/catlsvcs.catl.local complete, now 0 downloads active Aug 7 12:16:31 gigamonTA100 mgmtd[1130]: [mgmtd.ERR]: Set commit return status: code 0x1, message: error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure **Failure of the trusted channel (Remote syslog via SSH)** Aug 7 12:11:17 gigamonTA100 pm[1129]: [pm.NOTICE]: Output from mgmtd (Management Daemon) (pid 1130): Error: cipher mismatch Aug 7 12:11:17 gigamonTA100 mgmtd[22113]: [mgmtd.ERROR]: SSH connection to cctl@192.168.1.152:514 Encryption cipher mismatch

	Failure of the trusted channel (LDAP authentication server) Aug 7 12:03:03 gigamonTA100 sshd[21238]: pam_ldap: ldap_simple_bind: server ldap.catl.local:636: Can't contact LDAP server: sslv3 alert handshake failure
Initiation of the trusted path	**Initiation of the trusted path (SSH)** Jul 5 13:14:56 gigamonTA100 sshd[20980]: [INFO]: Postponed keyboard-interactive/pam for admin from 192.168.1.3 port 57516 ssh2 [preauth] Jul 5 13:14:56 gigamonTA100 sshd[20980]: [INFO]: Accepted keyboard-interactive/pam for admin from 192.168.1.3 port 57516 ssh2 Jul 5 13:14:56 gigamonTA100 sshd[20980]: [NOTICE]: User admin (System Administrator) logged in via ssh2 from 192.168.1.3 port 57516 **Initiation of the trusted path (TLS Web GUI)** Jul 5 13:36:43 gigamonTA100 wsmd[1328]: [wsmd.INFO]: Web session 2 created Jul 5 13:36:43 gigamonTA100 wsmd[1328]: [wsmd.INFO]: Recording web login of user admin on device /dev/web/2 Jul 5 13:36:43 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: Opened session: 58 Jul 5 13:36:43 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: session 58: opened for client wsmd.2-1328 user admin (0/0) 1 Jul 5 13:36:43 gigamonTA100 wsmd[1328]: [wsmd.INFO]: session 1: client open for peer mgmtd (local name wsmd.2-1328) Jul 5 13:36:43 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: TRUSTED_AUTH_INFO (user admin/admin): validated OK Jul 5 13:36:43 gigamonTA100 mgmtd[1147]: [mgmtd.NOTICE]: User admin (local user admin) authentication method: local Jul 5 13:36:43 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: EVENT: /mgmtd/session/events/login Jul 5 13:36:43 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: Calling internal interest callback for event /mgmtd/session/events/login Jul 5 13:36:43 gigamonTA100 mgmtd[1147]: [mgmtd.INFO]: Calling internal interest callback for event /mgmtd/session/events/login Jul 5 13:36:43 gigamonTA100 mgmtd[1147]: [mgmtd.NOTICE]: User admin: login from 192.168.1.98 through trusted web channel. Jul 5 13:36:43 gigamonTA100 wsmd[1328]: [wsmd.NOTICE]: User admin (System Administrator) logged into Web UI from 192.168.1.98
Termination of the trusted path	**Termination of the trusted path (SSH)** Jul 5 13:17:14 gigamonTA100 sshd[21230]: [INFO]: Received disconnect from 192.168.1.3: 11: disconnected by user

	Jul 5 13:17:14 gigamonTA100 sshd[21230]: pam_unix(sshd:session): session closed for user admin **Termination of the trusted path (TLS Web GUI)** Jul 5 13:37:33 gigamonTA100 wsmd[1328]: [wsmd.NOTICE]: User admin from 192.168.1.98 logged out of Web UI Jul 5 13:37:33 gigamonTA100 wsmd[1328]: [wsmd.INFO]: session 1: closing for peer mgmtd user i:1147-0-0 (0/0) 0 Jul 5 13:37:33 gigamonTA100 wsmd[1328]: [wsmd.INFO]: Web session 2 closed
Failure of the trusted path functions	**Failure of the trusted path functions (SSH)** Jul 5 13:25:34 gigamonTA100 sshd[21873]: [INFO (verbose)]: Connection from 192.168.1.3 port 57541 Jul 5 13:25:34 gigamonTA100 sshd[21873]: [FATAL]: no matching mac found: client hmac-md5 server hmac-sha1,hmac-sha2-256,hmac-sha2-512 [preauth] **Failure of the trusted path functions (TLS Web GUI)** Jul 5 13:38:25 gigamonTA100 httpd[26802]: [Thu Jul 05 13:38:25 2018] [error] [client 192.168.1.98] SSL library error 1 in handshake (server gigamonTA100:443) Jul 5 13:38:25 gigamonTA100 httpd[26802]: [Thu Jul 05 13:38:25 2018] [error] SSL Library Error: 336109761 error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher Too restrictive SSLCipherSuite or using DSA server certificate?

Table 9-1: Sample Audit Records