Assurance Activity Report for
Kemp LoadMaster

Kemp LoadMaster Security Target
Version 0.8

collaborative Protection Profile for Network Devices
Version 2.2e

collaborative Protection Profile for Network Devices

AAR v0.5, January 24, 2023

Evaluated by:

intertek
acumen
security

**2400 Research Blvd, Suite 395
Rockville, MD 20850**

**Prepared for:
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme**

The Developer of the TOE:
Progress Software Corporation

The Author of the Security Target:
Acumen Security, LLC

The TOE Evaluation was Sponsored by:
Progress Software Corporation

Evaluation Personnel:
Rahul Joshi
Yogesh Pawar
Shaunak Shah
Adarsh Pandey
Yogita Kore

Common Criteria Version

Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version

CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
0.1	7/13/2020	Initial Release
0.2	9/9/2020	Updated based on Kemp input
0.3	12/16/2022	Updated based on review comments
0.4	01/19/2023	Updated based on ECR comments
0.5	01/24/2023	Minor update

Table of Contents

1 TOE Overview 11
1.1 Evaluated Configuration 11
1.2 Physical Boundaries 11
1.3 Logical Boundaries 11
1.4 Excluded Functionality 13
2 Assurance Activities Identification 14
3 Test Equivalency Justification 15
3.1 Platform/Hardware Dependencies 15
3.2 Software/OS Dependencies: 15
3.3 Differences in Libraries Used to Provide TOE Functionality 16
3.4 TOE Management Interface Differences 16
3.5 TOE Functional Differences 16
3.6 Difference Comparison 16
3.7 Recommendations/Conclusions 16
4 Test Bed Descriptions 17
5 Detailed Test Cases (TSS and Guidance Activities) 19
5.1 TSS and Guidance Activities (Auditing) 19
5.1.1 FAU_GEN.1 19
5.1.1.1 FAU_GEN.1 TSS 1 19
5.1.1.2 FAU_GEN.1 Guidance 1 19
5.1.1.3 FAU_GEN.1 Guidance 2 19
5.1.2 FAU_STG_EXT.1 21
5.1.2.1 FAU_STG_EXT.1 TSS 1 21
5.1.2.2 FAU_STG_EXT.1 TSS 2 21
5.1.2.3 FAU_STG_EXT.1 TSS 3 21
5.1.2.4 FAU_STG_EXT.1 TSS 4 22
5.1.2.5 FAU_STG_EXT.1 TSS 5 22
5.1.2.6 FAU_STG_EXT.1 Guidance 1 23
5.1.2.7 FAU_STG_EXT.1 Guidance 2 23
5.1.2.8 FAU_STG_EXT.1 Guidance 3 23
5.1.3 FAU_STG_EXT.3/LocSpace 24
5.1.3.1 FAU_STG_EXT.3/LocSpace TSS 1 24
5.1.3.2 FAU_STG_EXT.3/LocSpace Guidance 1 24
5.2 TSS and Guidance Activities (Cryptographic Support) 25
5.2.1 FCS_CKM.1 25
5.2.1.1 FCS_CKM.1 TSS 1 25
5.2.1.2 FCS_CKM.1 Guidance 1 25
5.2.1.3 FCS_CKM.1 Test/CAVP 1 25
5.2.2 FCS_CKM.2 25
5.2.2.1 FCS_CKM.2 TSS 1 **[TD0580]** 25
5.2.2.2 FCS_CKM.2 Guidance 1 26
5.2.2.3 FCS_CKM.2 Test/CAVP 1 26
5.2.3 FCS_CKM.4 26
5.2.3.1 FCS_CKM.4 TSS 1 26
5.2.3.2 FCS_CKM.4 TSS 2 27

5.2.3.3 FCS_CKM.4 TSS 3 ... 28
5.2.3.4 FCS_CKM.4 TSS 4 ... 28
5.2.3.5 FCS_CKM.4 TSS 5 ... 29
5.2.3.6 FCS_CKM.4 Guidance 1 ... 29
5.2.4 FCS_COP.1/DataEncryption ... 29
5.2.4.1 FCS_COP.1/DataEncryption TSS 1 ... 29
5.2.4.2 FCS_COP.1/DataEncryption Guidance 1 ... 29
5.2.4.3 FCS_COP.1/DataEncryption Test/CAVP 1 ... 30
5.2.5 FCS_COP.1/SigGen ... 30
5.2.5.1 FCS_COP.1/SigGen TSS 1 ... 30
5.2.5.2 FCS_COP.1/SigGen Guidance 1 ... 30
5.2.5.3 FCS_COP.1/SigGen Test/CAVP 1 ... 31
5.2.6 FCS_COP.1/Hash ... 31
5.2.6.1 FCS_COP.1/Hash TSS 1 ... 31
5.2.6.2 FCS_COP.1/Hash Guidance 1 ... 31
5.2.6.3 FCS_COP.1/Hash Test/CAVP 1 ... 32
5.2.7 FCS_COP.1/KeyedHash ... 32
5.2.7.1 FCS_COP.1/KeyedHash TSS 1 ... 32
5.2.7.2 FCS_COP.1/KeyedHash Guidance 1 ... 32
5.2.7.3 FCS_COP.1/KeyedHash Test/CAVP 1 ... 33
5.2.8 FCS_RBG_EXT.1 ... 33
5.2.8.1 FCS_RBG_EXT.1 TSS 1 ... 33
5.2.8.2 FCS_RBG_EXT.1 Guidance 1 ... 33
5.2.8.3 FCS_RBG_EXT.1.1 Test/CAVP 1 ... 33
5.3 TSS and Guidance Activities (HTTPS) ... 34
5.3.1 FCS_HTTPS_EXT.1 ... 34
5.3.1.1 FCS_HTTPS_EXT.1.1 TSS 1 ... 34
5.3.1.2 FCS_HTTPS_EXT.1.1 Guidance 1 ... 34
5.4 TSS and Guidance Activities (NTP) ... 34
5.4.1 FCS_NTP_EXT.1 ... 34
5.4.1.1 FCS_NTP_EXT.1 TSS 1 ... 34
5.4.1.2 FCS_NTP_EXT.1 TSS 2 ... 35
5.4.1.3 FCS_NTP_EXT.1.1 Guidance 1 ... 35
5.4.1.4 FCS_NTP_EXT.1.2 Guidance 1 ... 35
5.4.1.5 FCS_NTP_EXT.1.3 Guidance 1 ... 36
5.5 TSS and Guidance Activities (TLS) ... 36
5.5.1 FCS_TLSC_EXT.1 ... 36
5.5.1.1 FCS_TLSC_EXT.1.1 TSS 1 ... 36
5.5.1.2 FCS_TLSC_EXT.1.1 Guidance 1 ... 37
5.5.1.3 FCS_TLSC_EXT.1.2 TSS 1 ... 37
5.5.1.4 FCS_TLSC_EXT.1.2 TSS 2 ... 37
5.5.1.5 FCS_TLSC_EXT.1.2 Guidance 1 ... 38
5.5.1.6 FCS_TLSC_EXT.1.4 TSS 1 ... 39
5.5.1.7 FCS_TLSC_EXT.1.4 Guidance 1 ... 39
5.5.2 FCS_TLSS_EXT.1 ... 40
5.5.2.1 FCS_TLSS_EXT.1.1 TSS 1 ... 40
5.5.2.2 FCS_TLSS_EXT.1.1 Guidance 1 ... 40
5.5.2.3 FCS_TLSS_EXT.1.2 TSS 1 ... 40
5.5.2.4 FCS_TLSS_EXT.1.2 Guidance 1 ... 41

5.5.2.5 FCS_TLSS_EXT.1.3 TSS 1 41
5.5.2.6 FCS_TLSS_EXT.1.3 Guidance 1 41
5.5.2.7 FCS_TLSS_EXT.1.4 TSS 1 41
5.5.2.8 FCS_TLSS_EXT.1.4 TSS 2 42
5.5.2.9 FCS_TLSS_EXT.1.4 TSS 3 42
5.5.2.10 FCS_TLSS_EXT.1.4 TSS 4 **[TD0569]** 42
5.6 TSS and Guidance Activities (Identification and Authentication) 43
5.6.1 FIA_AFL.1 43
5.6.1.1 FIA_AFL.1 TSS 1 43
5.6.1.2 FIA_AFL.1 TSS 2 43
5.6.1.3 FIA_AFL.1 Guidance 1 43
5.6.1.4 FIA_AFL.1 Guidance 2 44
5.6.2 FIA_PMG_EXT.1 44
5.6.2.1 FIA_PMG_EXT.1.1 TSS 1 44
5.6.2.2 FIA_PMG_EXT.1.1 Guidance 1 45
5.6.3 FIA_UIA_EXT.1 45
5.6.3.1 FIA_UIA_EXT.1 TSS 1 45
5.6.3.2 FIA_UIA_EXT.1 TSS 2 45
5.6.3.3 FIA_UIA_EXT.1 Guidance 1 46
5.6.4 FIA_UAU.7 46
5.6.4.1 FIA_UAU.7 Guidance 1 46
5.6.5 FIA_X509_EXT.1/Rev 46
5.6.5.1 FIA_X509_EXT.1/Rev TSS 1 46
5.6.5.2 FIA_X509_EXT.1/Rev TSS 2 47
5.6.5.3 FIA_X509_EXT.1/Rev Guidance 1 48
5.6.6 FIA_X509_EXT.2 48
5.6.6.1 FIA_X509_EXT.2 TSS 1 48
5.6.6.2 FIA_X509_EXT.2 TSS 2 48
5.6.6.3 FIA_X509_EXT.2 Guidance 1 49
5.6.6.4 FIA_X509_EXT.2 Guidance 2 49
5.6.6.5 FIA_X509_EXT.2 Guidance 3 49
5.6.7 FIA_X509_EXT.3 50
5.6.7.1 FIA_X509_EXT.3 TSS 1 50
5.6.7.2 FIA_X509_EXT.3 Guidance 1 50
5.7 TSS and Guidance Activities (Security Management) 50
5.7.1 FMT_MOF.1/ManualUpdate 50
5.7.1.1 FMT_MOF.1/ManualUpdate Guidance 1 50
5.7.2 FMT_MTD.1/CoreData 51
5.7.2.1 FMT_MTD.1/CoreData TSS 1 51
5.7.2.2 FMT_MTD.1/CoreData TSS 2 51
5.7.2.3 FMT_MTD.1/CoreData Guidance 1 51
5.7.2.4 FMT_MTD.1/CoreData Guidance 2 52
5.7.3 FMT_MTD.1/CryptoKeys 53
5.7.3.1 FMT_MTD.1/CryptoKeys TSS 1 53
5.7.3.2 FMT_MTD.1/CryptoKeys Guidance 1 53
5.7.4 FMT_SMF.1 54
5.7.4.1 FMT_SMF.1 TSS 1 54
5.7.4.2 FMT_SMF.1 Guidance 1 54
5.7.5 FMT_SMR.2 55

5.7.5.1 FMT_SMR.2 TSS 1 55
5.7.5.2 FMT_SMR.2 Guidance 1........55
5.8 TSS and Guidance Activities (Protection of the TSF) 55
5.8.1 FPT_APW_EXT.1........55
5.8.1.1 FPT_APW_EXT.1 TSS 1 55
5.8.2 FPT_SKP_EXT.1........56
5.8.2.1 FPT_SKP_EXT.1 TSS 1 56
5.8.3 FPT_STM_EXT.1........56
5.8.3.1 FPT_STM_EXT.1 TSS 1 56
5.8.3.2 FPT_STM_EXT.1 Guidance 1 57
5.8.4 FPT_TST_EXT.1.1........57
5.8.4.1 FPT_TST_EXT.1.1 TSS 1 57
5.8.4.2 FPT_TST_EXT.1.1 Guidance 1........58
5.8.5 FPT_TUD_EXT.1........58
5.8.5.1 FPT_TUD_EXT.1 TSS 1 58
5.8.5.2 FPT_TUD_EXT.1 TSS 2 58
5.8.5.3 FPT_TUD_EXT.1 TSS 3 59
5.8.5.4 FPT_TUD_EXT.1 Guidance 1........60
5.8.5.5 FPT_TUD_EXT.1 Guidance 2........60
5.8.5.6 FPT_TUD_EXT.1 Guidance 3........60
5.8.5.7 FPT_TUD_EXT.1 Guidance 4........60
5.9 TSS and Guidance Activities (TOE Access) 61
5.9.1 FTA_SSL_EXT.1 61
5.9.1.1 FTA_SSL_EXT.1 TSS 1........61
5.9.1.2 FTA_SSL_EXT.1 Guidance 1 61
5.9.2 FTA_SSL.3 61
5.9.2.1 FTA_SSL.3 TSS 1 61
5.9.2.2 FTA_SSL.3 Guidance 1........62
5.9.3 FTA_SSL.4 62
5.9.3.1 FTA_SSL.4 TSS 1 62
5.9.3.2 FTA_SSL.4 Guidance 1........62
5.9.4 FTA_TAB.1 62
5.9.4.1 FTA_TAB.1 TSS 1 62
5.9.4.2 FTA_TAB.1 Guidance 1........63
5.10 TSS and Guidance Activities (Trusted Path/Channels) 63
5.10.1 FTP_ITC.1........63
5.10.1.1 FTP_ITC.1 TSS 1 63
5.10.1.2 FTP_ITC.1 Guidance 1 64
5.10.2 FTP_TRP.1/Admin 64
5.10.2.1 FTP_TRP.1/Admin TSS 1........64
5.10.2.2 FTP_TRP.1/Admin Guidance 1 64
6 Detailed Test Cases (Test Activities)........66
NDcPP Test Cases........66
6.1 FAU_GEN.1 Test #1 66
6.2 FAU_STG_EXT.1 Test #1 74
6.3 FAU_STG_EXT.1 Test #2b 74
6.4 FAU_STG_EXT.3/LocSpace 75
6.5 FCS_NTP_EXT.1.1 Test #1 75

6.6 FCS_NTP_EXT.1.2 Test #1 76

6.7 FCS_NTP_EXT.1.3 Test #1 76

6.8 FCS_NTP_EXT.1.4 Test #1 77

6.9 FCS_NTP_EXT.1.4 Test #2 78

6.10 FPT_STM_EXT.1 Test #1 78

6.11 FPT_STM_EXT.1 Test #2 78

6.12 FTP_ITC.1 Test #1 79

6.13 FTP_ITC.1 Test #2 79

6.14 FTP_ITC.1 Test #3 79

6.15 FTP_ITC.1 Test #4 79

6.16 FCS_HTTPS_EXT.1 Test#1 80

6.17 FIA_AFL.1 Test #1 80

6.18 FIA_AFL.1 Test #2a 81

6.19 FIA_PMG_EXT.1 Test #1 81

6.20 FIA_PMG_EXT.1 Test #2 82

6.21 FIA_UIA_EXT.1 Test #1 83

6.22 FIA_UIA_EXT.1 Test #2 83

6.23 FIA_UIA_EXT.1 Test #3 84

6.24 FIA_UAU.7 Test #1 84

6.25 FMT_MOF.1/ManualUpdate Test #1 85

6.26 FMT_MOF.1/ManualUpdate Test #2 85

6.27 FMT_MTD.1/CryptoKeys Test #1 85

6.28 FMT_MTD.1/CryptoKeys Test #2 86

6.29 FMT_SMF.1 Test #1 86

6.30 FMT_SMR.2 Test #1 87

6.31 FTA_SSL.3 Test #1 87

6.32 FTA_SSL.4 Test #1 88

6.33 FTA_SSL.4 Test #2 88

6.34 FTA_SSL_EXT.1.1 Test #1 88

6.35 FTA_TAB.1 Test #1 89

6.36 FTP_TRP.1/Admin Test #1 89

6.37 FTP_TRP.1/Admin Test #2 90

6.38 FCS_TLSC_EXT.1.1 Test #1 90

6.39 FCS_TLSC_EXT.1.1 Test #2 91

6.40 FCS_TLSC_EXT.1.1 Test #3 91

6.41 FCS_TLSC_EXT.1.1 Test #4a 91

6.42 FCS_TLSC_EXT.1.1 Test #4b 92

6.43 FCS_TLSC_EXT.1.1 Test #4c 92

6.44 FCS_TLSC_EXT.1.1 Test #5a 92

6.45 FCS_TLSC_EXT.1.1 Test #5b 93

6.46 FCS_TLSC_EXT.1.1 Test #6a 93

6.47 FCS_TLSC_EXT.1.1 Test #6b 93

6.48 FCS_TLSC_EXT.1.1 Test #6c 94

6.49 FCS_TLSC_EXT.1.2 Test #1 94

6.50 FCS_TLSC_EXT.1.2 Test #2 95

6.51 FCS_TLSC_EXT.1.2 Test #3 95

6.52 FCS_TLSC_EXT.1.2 Test #4 96
6.53 FCS_TLSC_EXT.1.2 Test #5 (1) 97
6.54 FCS_TLSC_EXT.1.2 Test #5 (2)(a) 97
6.55 FCS_TLSC_EXT.1.2 Test #5 (2)(b) 98
6.56 FCS_TLSC_EXT.1.2 Test #5 (2)(c) 99
6.57 FCS_TLSC_EXT.1.2 Test #6 99
6.58 FCS_TLSC_EXT.1.3 Test #1 100
6.59 FCS_TLSC_EXT.1.3 Test #2 100
6.60 FCS_TLSC_EXT.1.3 Test #3 101
6.61 FCS_TLSC_EXT.1.4 Test #1 101
6.62 FCS_TLSS_EXT.1.1 Test #1 102
6.63 FCS_TLSS_EXT.1.1 Test #2 103
6.64 FCS_TLSS_EXT.1.1 Test #3a........ 103
6.65 FCS_TLSS_EXT.1.1 Test #3b 103
6.66 FCS_TLSS_EXT.1.2 Test #1 104
6.67 FCS_TLSS_EXT.1.3 Test #1a........ 105
6.68 FCS_TLSS_EXT.1.3 Test #1b 105
6.69 FCS_TLSS_EXT.1.4 Test #1 106
6.70 FPT_TST_EXT.1 Test #1........ 106
6.71 FPT_TUD_EXT.1 Test #1 107
6.72 FPT_TUD_EXT.1 Test #2 (a) 107
6.73 FPT_TUD_EXT.1 Test #2 (b) 108
6.74 FPT_TUD_EXT.1 Test #2 (c)........ 109
6.75 FIA_X509_EXT.1.1/Rev Test #1a 109
6.76 FIA_X509_EXT.1.1/Rev Test #1b........ 110
6.77 FIA_X509_EXT.1.1/Rev Test #2........ 110
6.78 FIA_X509_EXT.1.1/Rev Test #3........ 110
6.79 FIA_X509_EXT.1.1/Rev Test #4........ 111
6.80 FIA_X509_EXT.1.1/Rev Test #5........ 112
6.81 FIA_X509_EXT.1.1/Rev Test #6........ 112
6.82 FIA_X509_EXT.1.1/Rev Test #7........ 113
6.83 FIA_X509_EXT.1.1/Rev Test #8a 113
6.84 FIA_X509_EXT.1.1/Rev Test #8b........ 113
6.85 FIA_X509_EXT.1.1/Rev Test #8c 114
6.86 FIA_X509_EXT.1.2/Rev Test #1........ 114
6.87 FIA_X509_EXT.1.2/Rev Test #2........ 115
6.88 FIA_X509_EXT.2 Test #1 116
6.89 FIA_X509_EXT.3 Test #1 117
6.90 FIA_X509_EXT.3 Test #2 117
7 Security Assurance Requirements........ 119
7.1 ADV_FSP.1 Basic Functional Specification........ 119
7.1.1 ADV_FSP.1 119
7.1.1.1 ADV_FSP.1 Activity 1........ 119
7.1.1.2 ADV_FSP.1 Activity 2........ 119
7.1.1.3 ADV_FSP.1 Activity 3........ 119
7.2 AGD_OPE.1 Operational User Guidance 119

7.2.1 AGD_OPE.1 119
7.2.1.1 AGD_OPE.1 Activity 1 119
7.2.1.2 AGD_OPE.1 Activity 2 120
7.2.1.3 AGD_OPE.1 Activity 3 120
7.2.1.4 AGD_OPE.1 Activity 4 120
7.2.1.5 AGD_OPE.1 Activity 5 **[TD0536]** 121
7.3 AGD_PRE.1 Preparative Procedures 121
7.3.1 AGD_PRE.1 121
7.3.1.1 AGD_PRE.1 Activity 1 121
7.3.1.2 AGD_PRE.1 Activity 2 122
7.3.1.3 AGD_PRE.1 Activity 3 122
7.3.1.4 AGD_PRE.1 Activity 4 123
7.3.1.5 AGD_PRE.1 Activity 5 123
7.4 ALC Assurance Activities 123
7.4.1 ALC_CMC.1 123
7.4.1.1 ALC_CMC.1 Activity 1 123
7.4.2 ALC_CMS.1 124
7.4.2.1 ALC_CMS.1 Activity 1 124
7.5 ATE_IND.1 Independent Testing – Conformance 124
7.5.1 ATE_IND.1 124
7.5.1.1 ATE_IND.1 Activity 1 124
7.6 AVA_VAN.1 Vulnerability Survey 124
7.6.1 AVA_VAN.1 124
7.6.1.1 AVA_VAN.1 Activity 1 **[TD0564, Labgram #116]** 124
7.6.1.2 AVA_VAN.1 Activity 2 125
8 Conclusion 127

1 TOE Overview

The TOE is Kemp LoadMaster X15, X25 and X40 and Virtual LoadMaster both running on OS 7.2.48.8. The LoadMaster simplifies the management of networked resources, and optimizes and accelerates user access to diverse servers, content, and transaction-based systems. The TOE is comprised of hardware and software and represents a complete network device providing load balancing functionality.

1.1 Evaluated Configuration

The TOE supports (sometimes optionally) secure connectivity with several other IT environment devices as described below.

Component	Required	Usage/Purpose Description
Management Workstation	Yes	Workstation providing local console access to the TOE. Workstation providing a browser to connected to the Web User Interface (WUI) over TLSv1.2 or TLSv1.1.
Audit Server	Yes	Syslog server that receives audit logs from the TOE over TLSv1.2 or TLSv1.1.
ESXi Server	Yes (for Virtual LoadMaster)	ESXi v6.7 acting as the hypervisor for Virtual LoadMaster.
LDAP Server	No	Optional authentication server supporting LDAP over TLSv1.2 or TLSv1.1.
NTP Server	No	Optional NTP server supporting SHA-1 integrity verification.

Table 1 IT Environment Components

1.2 Physical Boundaries

The TOE boundary consists of one of the appliances listed below. The LoadMaster X15, X25 and X40 are physical devices while the Virtual LoadMaster is a virtual machine which runs on ESXi. The virtual TOE is conformant with Case 1 as described in the NDcPP:

Model	LoadMaster X15	LoadMaster X25	LoadMaster X40	Virtual LoadMaster
Processor	Intel Xeon E3-1275v6 (Kaby Lake)	Intel Xeon Silver 4116T (Skylake)	Intel Xeon Gold 6136 (Skylake)	Intel Xeon E5 4620 v4 (Broadwell)
RAM	32 GB RAM	64 GB RAM	64 GB RAM	2GB (evaluated)
Network	16 1Gb Ethernet 4 10Gb Ethernet Fiber	2 1Gb Ethernet 12 10Gb Ethernet Fiber	2 1Gb Ethernet 12 10Gb Ethernet Fiber	3 1Gb virtual NIC (evaluated)
Platform	**Error! Unknown document property name.**8	**Error! Unknown document property name.**8	**Error! Unknown document property name.**8	**Error! Unknown document property name.**8 on ESXi v6.7

Table 2 IT Environment Components

The Virtual LoadMaster was tested on an Intel Xeon E5-4620v4 (Broadwell) and ESXi v6.7.

1.3 Logical Boundaries

The TOE provides the security functionality required by [NDcPP].

- **Security Audit**

The TOE generates audit records for security relevant events. The audit events are associated with the administrator or processes. The audit records are transmitted over TLS to an external audit server.

- **Cryptographic Support**

The TOE utilizes the LoadMaster FIPS Object Module v1.0 (FIPS Cert. #3736) for cryptographic services described below.

Service	Use
TLS Client	Secure connection to remote syslog servers.
TLS Client	Secure connection to remote LDAP server.
TLS/HTTPS Server	Secures connections with remote administrators.
Verification of Updates	Digital signature verification prior to installing an update.

Table 3 Cryptographic Services

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below.

Algorithm	CAVP Cert.	Standard	Operation/Use	SFR
RSA	C2076	FIPS 186-4	RSA 2048 SigVer	FCS_CKM.1
ECDSA	C2076	FIPS 186-4	ECDSA P-256 SigGen, SigVer ECDSA P-256, P-384, P-521 KeyGen, PKV	FCS_CKM.1 FCS_COP.1/SigGen
ECDHE	C2076	SP 800-56Ar2	ECDHE P-256, P-384, P-521	FCS_CKM.2
DRBG	C2076	SP 800-90Ar1	CTR_DRBG(AES-256)	FCS_RBG_EXT.1
AES	C2076	FIPS 197 SP 800-38A SP 800-38D	AES in CBC and GCM modes with 128-bit and 256-bit keys	FCS_COP.1/DataEncryption
SHA	C2076	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512	FCS_COP.1/Hash
HMAC	C2076	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	FCS_COP.1/Keyed Hash

Table 4 CAVP Algorithm Testing References

- **Identification and Authentication**

The TOE provides password-based and X.509 certificate-based logon mechanisms. This password-based mechanism encores minimum length requirements. The TOE also validates and authenticates X.509 certificates when they are used to identify a remote TLS server or an administrator logging into the TOE.

- **Security Management**

The TOE provides management capabilities via a Web-based GUI, accessed over HTTPS. Management functions allow the administrators to configure the system, install updates, and manage users.

- **Protection of the TSF**

The TOE prevents the reading of plaintext passwords and keys. The TOE provides a reliable timestamp for its own use. The reliable timestamp can be set by a security administrator or authenticated NTP. To protect the integrity of its security functions, the TOE implements a suite of self-tests at startup and halts or disables affected functionality if a self-test fails. The TOE ensures that updates to the TOE are authenticated by verifying a digital signature prior to installing any update.

- **TOE access**

The TOE monitors local and remote administrative sessions for inactivity and either locks or terminates the session when a threshold time period is reached. An advisory notice is displayed at the start of each session.

- **Trusted Path/Channels**

The TOE initiates a TLS trusted channel with a syslog server and LDAP authentication server (as configured). The TOE is a TLS/HTTPS server that allows remote administrators to establish a trusted path with the TOE.

1.4 Excluded Functionality

The following functionality is excluded (disabled) in the evaluated configuration:

- SSH
- Management API
- Administrative Trusted Channels
- IPv6

2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the NDcPP 2.2e based upon the core SFRs and those implemented based on selections within the PPs/EPs.

3 Test Equivalency Justification

The following equivalency analysis provides a per category analysis of key areas of differentiation for each hardware model to determine the minimum subset to be used in testing. The areas examined will use the areas and analysis description provided in the supporting documentation for the NDcPPv2.2e. Additionally, a comparison of the data presented in section 3 is provided to identify a testing subset that will exercise each of the differences in TOE models.

3.1 Platform/Hardware Dependencies

The TOE boundary is inclusive of all hardware required by the TOE. The hardware platforms do not provide any of the TSF functionality. The hardware within the TOE only differs by configuration and performance.

Model	LoadMaster X15	LoadMaster X25	LoadMaster X40	Virtual LoadMaster
Processor	Intel Xeon E3-1275v6 (Kaby Lake)	Intel Xeon Silver 4116T (Skylake)	Intel Xeon Gold 6136 (Skylake)	Intel Xeon E5 4620 v4 (Broadwell)
RAM	32 GB RAM	64 GB RAM	64 GB RAM	2GB (evaluated)
Network	16 1Gb Ethernet 4 10Gb Ethernet Fiber	2 1Gb Ethernet 12 10Gb Ethernet Fiber	2 1Gb Ethernet 12 10Gb Ethernet Fiber	3 1Gb virtual NIC (evaluated)
Platform	Loadmaster OS 7.2.48.8	Loadmaster OS 7.2.48.8	Loadmaster OS 7.2.48.8	Loadmaster OS 7.2.48.8 on ESXi v6.7

The TOE chassis includes varying form factors. Although the chassis may differ, it does not affect the functionality of the TOE.

Result: All platforms are equivalent.

3.2 Software/OS Dependencies:

The underlying OS is installed with the application-level software on each of the devices. The LMOS software has version 7.2.48.8. The LMOS software can run on a dedicated hardware appliances and on servers running on ESXi 6.7 hypervisor. All models include the same security functionality. There are no specific dependencies on the OS apart from the additional hypervisor layer in case of virtual model.

TOE Model	Description	Analysis
Operating System – This is the OS that runs on the platform		
LoadMaster X15	Loadmaster OS 7.2.48.8	All three hardware devices are running the same OS and installed using the same image. The virtual TOE is also running the same OS but on ESXi v6.7 hypervisor. Verdict: The three hardware models are equivalent.
LoadMaster X25	Loadmaster OS 7.2.48.8	
LoadMaster X40	Loadmaster OS 7.2.48.8	
Virtual LoadMaster	Loadmaster OS 7.2.48.8 on ESXi v6.7	

Result :

- All Hardware models are equivalent. One of the three hardware models will be tested.
- One virtual model will be tested.

3.3 Differences in Libraries Used to Provide TOE Functionality

All software binaries compiled in the TOE software are identical and have the same version numbers. There are no differences between the included libraries. Of note, the TOE uses the same cryptographic module to provide its cryptographic functionality. This is the same across platforms.

Result :

- There are no differences in the included libraries.
- All models are equivalent.

3.4 TOE Management Interface Differences

The TOE is managed via either remote CLI session or directly connected CLI. These management options are available on all hardware platforms regardless of the configuration. There is no difference in the management interface for any platform.

Result: All models are equivalent

3.5 TOE Functional Differences

Each hardware model within the TOE boundary provides identical functionality. There is no difference in the way the user interacts with each of the devices or the services that are available to the user in for each of these devices. Each device runs the same version of LoadMaster OS. If there had been differences in the functionality provided by the software, the actual release version would have been different for the platform.

Result: All models are equivalent

3.6 Difference Comparison

All platforms run the same software and perform identical functionality. All hardware platforms use identical microarchitecture processors. The virtual model uses a different microarchitecture processor.

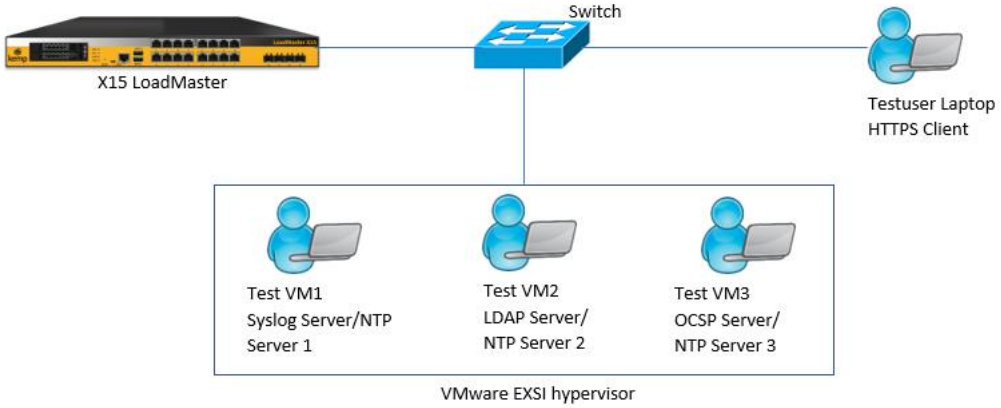
3.7 Recommendations/Conclusions

Based on the equivalency rationale listed above, testing will be performed on the following subset,

- One of the three hardware models will be tested:
  - LoadMaster X15 was selected to be tested
- One virtual model will be tested:
  - Virtual LoadMaster running on ESXi v6.7 was selected to be tested

4 Test Bed Descriptions

TEST BED Audit/Auth/TLSC/TLSS/Update/X509:



LABGRAM:

Name	OS	Function	Protocol	Time	Tools (version)
X15 LoadMaster	LoadMaster OS v7.2.48.8	TOE	TLS/HTTPS	Manually set and verified	NA
Virtual LoadMaster	LoadMaster OS v7.2.48.8	TOE	TLS/HTTPS	Manually set and verified	N/A
VMware EXSI hypervisor	ESXi-6.7	Console	HTTPS	Manually set and verified	NA
Console Server	Wakko-Console	Console	Console	Manually set and verified	NA
Test User Laptop	Windows10	Test Workstation,	SSH/ICMP	Manually set and verified	Wireshark v3.03; Firefox Browser 91.0.1, MobaXTerm v11.0, PuTTy v0.70, Hex Editor Version 1.9.0
Syslog Server/NTP Server 1	Ubuntu 18.04.5 LTS	Ubuntu 18.04.5 LTS	TLS/HTTPS/NTP	Manually set and verified	Openssl (s_server) (s_client)1.1.1 XCAv2.1.1; Rsyslogd 8.32.0 acumen-tlsc, acumen-tlss-v2.2e
LDAP Server/ NTP Server 2	Ubuntu 18.04 LTS	Authentication Server, Time synchronization server	TLS/NTP	Synced with NTP	ntpd 4.2.8, Server Manager 10.0.14393.2608 Certification Authority 10.0

Name	OS	Function	Protocol	Time	Tools (version)
NTP Server 3	Ubuntu 18.04 LTS	Time synchronization server	TLS/NTP	Synced with NTP	ntpd 4.2.8
OCSP Server	Ubuntu 20.04.2 LTS	OCSP Server	TLS	Synced with NTP	Openssl(s_server)(s_clinet)1.1.1

5 Detailed Test Cases (TSS and Guidance Activities)

5.1 TSS and Guidance Activities (Auditing)

5.1.1 FAU_GEN.1

5.1.1.1 FAU_GEN.1 TSS 1

Objective	For the administrative task of generating/import of, changing, or deleting of cryptographic keys as defined in FAU_GEN.1.1c, the TSS should identify what information is logged to identify the relevant key.
Evaluator Findings	The evaluator examined the **FAU_GEN.1** entry in section titled **TOE Summary Specification** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that within this section it identified the following information that was logged in order to identify the relevant key in relation to import/generation, changing, or deletion of cryptographic keys: **The TSF generates audit records for the auditable events specified in as well as the following:** • **Startup and shut-down of the audit function** • **Generation/importing, changing, or deleting certificates and cryptographic keys. The TSF identifies the certificate or key being operated on by including the following in the audit record:** ○ **Generated Keys:** ▪ **CSRs: X.509 Subject associated with the key** ▪ **Self-Signed Cert: hostname (in the CN)** ○ **Uploaded/Imported Keys: uploaded filename or certificate name.** ○ **For changing, and deleting of certificates and associated keys, the TOE logs the certificate name.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.2 FAU_GEN.1 Guidance 1

Objective	The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by FAU_GEN.1 (i.e., at least one instance of each auditable event, comprising the mandatory, optional and selection based SFR sections as applicable, shall be provided from the actual audit record).
Evaluator Findings	The evaluator examined the section titled **Sample Audit Logs** in the AGD to verify that it provides an example of each auditable event required by FAU_GEN.1. Upon investigation, the evaluator found that the AGD includes an example of the applicable audit events. There are no missing examples of auditable activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.3 FAU_GEN.1 Guidance 2

Objective	The evaluator shall also make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including

<table>
<tr><td></td><td>enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are related to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.</td></tr>
<tr><td>Evaluator Findings</td><td>
<p>The evaluator examined the AGD to verify that it identifies administrative commands, including subcommands, scripts, and configuration files, that are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator first examined the entirety of AGD to determine what administrative commands are associated with each administrative activity. Upon investigation, the evaluator found that the following are applicable:</p>
<table>
<tr><th>Administrative Activity</th><th>Method (Command/GUI Configuration)</th><th>Section</th></tr>
<tr><td><b>Audit configuration</b></td><td>Graphical User Interface</td><td>Section Titled:
<b>‘Syslog’</b></td></tr>
<tr><td><b>User Creation</b></td><td>Graphical User Interface</td><td>Section Titled:
<b>‘User Creation’</b></td></tr>
<tr><td><b>Software update</b></td><td>Graphical User Interface</td><td>Section Titled:
<b>‘Installing an Update Image’</b></td></tr>
<tr><td><b>Setting time</b></td><td>Graphical User Interface</td><td>Section Titled:
<b>‘Setting Date/Time’</b></td></tr>
<tr><td><b>Configuring banner</b></td><td>Graphical User Interface</td><td>Section Titled:
<b>‘Set the GUI Banner’</b>
<b>‘Set the CLI Banner’</b></td></tr>
</table>
<p>Next, the evaluator examined each of the test cases and identified test cases which exercised the above referenced functionality. The audit record associated with the configuration was captured. The following table identifies the test cases in which audit records for those configurations can be found.</p>
<table>
<tr><th>Administrative Activity</th><th>Method (Command/GUI Configuration)</th><th>Test Case(s)</th></tr>
<tr><td><b>Audit configuration</b></td><td>Graphical User Interface</td><td>FAU_STG_EXT.1 Test #1</td></tr>
<tr><td><b>User Creation</b></td><td>Graphical User Interface</td><td>FIA_PMG_EXT.1 Test#1</td></tr>
<tr><td><b>Software update</b></td><td>Graphical User Interface</td><td>FPT_TUD_EXT.1 Test #1</td></tr>
<tr><td><b>Setting time</b></td><td>Graphical User Interface</td><td>FPT_STM_EXT.1 Test #1</td></tr>
<tr><td><b>Configuring banner</b></td><td>Graphical User Interface</td><td>FTA_TAB.1 Test#1</td></tr>
</table>
</td></tr>
</table>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2 FAU_STG_EXT.1

5.1.2.1 FAU_STG_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.
Evaluator Findings	The evaluator examined the **FAU_STG_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Upon investigation, the evaluator found that the TSS states that: **The TSF transmits generated audit data to an external server using the TLS trusted channel specified in FTP_ITC.1. The TSF sends audit records to the external server as the audit records are generated. The TSF does not retransmit audit logs that were generated while the connection to the audit server was down.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.2 FAU_STG_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access.
Evaluator Findings	The evaluator examined the **FAU_STG_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. Upon investigation, the evaluator found that the TSS states that: **When local audit storage is exhausted, the TSF drops new audit records. The TSF allows all available space to be used to store audit records. For the Virtual Load Master that is up to 7GB. The HW Load Master models have up to 25GB of space available to store audit records.** **The TSF prevents unauthorized users from modifying or deleting audit records.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.3 FAU_STG_EXT.1 TSS 3

Objective	The evaluator shall examine the TSS to ensure it describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs it contains a list of TOE components that store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs that contain components which do not

	store audit data locally but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components.
Evaluator Findings	The evaluator examined the **FAU_STG_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. Upon investigation, the evaluator found that the TSS states that: **The TSF transmits generated audit data to an external server using the TLS trusted channel specified in FTP_ITC.1. The TSF sends audit records to the external server as the audit records are generated. The TSF does not retransmit audit logs that were generated while the connection to the audit server was down.** **The TOE is a standalone TOE.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.4 FAU_STG_EXT.1 TSS 4

Objective	The evaluator shall examine the TSS to ensure that it details the behavior of the TOE when the storage space for audit data is full. When the option 'overwrite previous audit record' is selected this description should include an outline of the rule for overwriting audit data. If 'other actions' are chosen such as sending the new audit data to an external IT entity, then the related behavior of the TOE shall also be detailed in the TSS.
Evaluator Findings	The evaluator examined the **FAU_STG_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS details the behavior of the TOE when the storage space for audit data is full. Upon investigation, the evaluator found that the TSS states that: **When local audit storage is exhausted, the TSF will not record new events locally until additional space is available. Records are still transmitted to the remote syslog endpoint, and so the audit trail is preserved. Local audit records will be temporarily stored in a buffer until they can be stored. The TSF allows all available space to be used to store audit records. For the Virtual Load Master that is up to 7GB. The HW Load Master models have up to 25GB of space available to store audit records..** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.5 FAU_STG_EXT.1 TSS 5

Objective	The evaluator shall examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. In case the TOE does not perform transmission in realtime the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data.
Evaluator Findings	The evaluator examined the **FAU_STG_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS details whether the transmission of

	audit information to an external IT entity can be done in realtime or periodically. Upon investigation, the evaluator found that the TSS states that: **The TSF sends audit records to the external server as the audit records are generated. The TSF does not retransmit audit logs that were generated while the connection to the audit server was down.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.6 FAU_STG_EXT.1 Guidance 1

Objective	The evaluator shall also examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.
Evaluator Findings	The evaluator examined the section titled **Secure Remote Logging** in the AGD to verify that it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server. Upon investigation, the evaluator found that the AGD includes a description of the protocols used to communicate with the server (TLS 1.1 or TLS 1.2) and the commands required to configure the TOE to connect to the remote audit server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.7 FAU_STG_EXT.1 Guidance 2

Objective	The evaluator shall also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and “cleared” periodically by sending the data to the audit server.
Evaluator Findings	The evaluator examined the section titled **Auditing** in the AGD to verify that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. Upon investigation, the evaluator found that the AGD states that sends audit records to the external server as the audit records are generated. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.8 FAU_STG_EXT.1 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.
Evaluator Findings	The evaluator examined the section titled **‘Appendix B: Generating Log Data for FAU_STG_EXT.1 Test #2’** in the AGD Appendix Document to verify that it describes all

	possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. Upon investigation, the evaluator found that the description of the available configuration options for handling a full local audit record as described in AGD. evaluator compared the exhausted local audit handling description found in AGD to the description provided by the TSS of the ST. The descriptions of the behavior found in AGD and ST are consistent. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3 FAU_STG_EXT.3/LocSpace

5.1.3.1 FAU_STG_EXT.3/LocSpace TSS 1

Objective	The evaluator shall examine the TSS to ensure that it details how the user is warned before the local storage for audit data is full.
Evaluator Findings	The evaluator examined **FAU_STG_EXT.3/LocSpace** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS details how the user is warned before the local storage for audit data is full. Upon investigation, the evaluator found that the TSS states that: **The TSF generates a log when audit storage reaches 85% of capacity to inform the administrator that audit storage is nearing capacity.** **The Disk Usage under System Configuration > System Administration > System Log Files provides a visual indication of the percentage used/free of the log partition. Color coding is used to highlight different usage levels:** **0% to 50%: green** **50% to 90%: orange** **90% to 100%: red** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.2 FAU_STG_EXT.3/LocSpace Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes how the user is warned before the local storage for audit data is full and how this warning is displayed or stored (since there is no guarantee that an administrator session is running at the time the warning is issued, it is probably stored in the log files). The description in the guidance documentation shall correspond to the description in the TSS.
Evaluator Findings	The evaluator examined the section titled **'Auditing'** in the AGD to verify that it describes how the user is warned before the local storage for audit data is full and how this warning is displayed or stored. Upon investigation, the evaluator found that the AGD shows how the user is warned with the storage capacity. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2 TSS and Guidance Activities (Cryptographic Support)

Note that Test activities in the SD that are typically addressed by referencing CAVP certs are addressed in this section and are identified as "Test/CAVP" activities.

5.2.1 FCS_CKM.1

5.2.1.1 FCS_CKM.1 TSS 1

Objective	The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.
Evaluator Findings	The evaluator examined **FCS_CKM.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies the key sizes supported by the TOE. Upon investigation, the evaluator found that the TSS states that: **The TSF generates P-256 ECDSA keys for the administrative UI (HTTPS). The TSF generates P-256, P-384, and P-521 ECDH for the ECDHE key establishment used in TLS.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.2 FCS_CKM.1 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target.
Evaluator Findings	The evaluator examined the section titled '**Set ECC Ciphers for Self-Signed Certificates and Outbound Connections'** in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target. Upon investigation, the evaluator found that the AGD states that the configuration for Self-Signed Certificates and CSR related keys for the webUI is described. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.3 FCS_CKM.1 Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: #C2076 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2 FCS_CKM.2

5.2.2.1 FCS_CKM.2 TSS 1 **[TD0580]**

Objective	The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS.

Evaluator Findings	The evaluator examined the **FCS_CKM.2** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. Upon investigation, the evaluator found that the TSS states that: **The TSF performs SP 800-56Ar2 compliant elliptic curve-based key establishment using curves P-256, P-384, and P-521 as part of the TLS handshake.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.2 FCS_CKM.2 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).
Evaluator Findings	The evaluator examined the sections titled **Admin WUI Access** and **Set ECC Ciphers for Self-Signed Certificates and Outbound Connections** in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD describes the guidance specifically states that when ECC ciphers and certificates are configured no additional configuration is required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.3 FCS_CKM.2 Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: #C2076 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3 FCS_CKM.4

5.2.3.1 FCS_CKM.4 TSS 1

Objective	The evaluator examines the TSS to ensure it lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g., factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. For the purpose of this Evaluation Activity the relevant keys are those keys that are relied upon to support any of the SFRs in the Security Target. The evaluator confirms that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g., that all keys for the TOE-specific secure channels and protocols, or that support FPT_APW.EXT.1 and FPT_SKP_EXT.1, are accounted for2). In particular, if a TOE claims not to store plaintext keys in non-volatile memory then the evaluator checks that this is consistent with the operation of the TOE.
Evaluator Findings	The evaluator examined the section titled **Key storage and zeroization** under **TOE summary and specification** in the Security Target to verify that the TSS lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g., factory reset or device wipe function, disconnection of trusted channels, key change as part of a

<table>
<tr><td></td><td>
<p>secure channel protocol), and the destruction method used in each case. Upon investigation, the evaluator found that the TSS states that:</p>
<table>
<tr><th>Key</th><th>Type</th><th>Origin</th><th>Storage/Protection</th><th>Zeroization</th></tr>
<tr><td>EC Diffie-Hellman Key</td><td>Private ECDH P-256, P-384, or P-521</td><td>TOE generated</td><td>RAM</td><td>Keys are overwritten with zeros when session closes</td></tr>
<tr><td>TLS Private Key</td><td>Private ECDSA P-256</td><td>TOE generated</td><td>Restricted Filesystem access</td><td>Zeroize command</td></tr>
<tr><td>TLS Encryption Key</td><td>128-bit or 256-bit AES</td><td>TOE generated</td><td>RAM</td><td>Keys are overwritten with zeros when session closes</td></tr>
<tr><td>TLS Integrity Key</td><td>HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384</td><td>TOE generated</td><td>RAM</td><td>Keys are overwritten with zeros when session closes</td></tr>
</table>
<p>The Evaluator found that the descriptions of keys and storage locations is consistent with the functions carried out by the TOE.</p>
<p>Based on these findings, this assurance activity is considered satisfied.</p>
</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

5.2.3.2 FCS_CKM.4 TSS 2

<table>
<tr><td>Objective</td><td>The evaluator shall check to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs).</td></tr>
<tr><td>Evaluator Findings</td><td>
<p>The evaluator examined the <b>FCS_CKM.4</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys. Upon investigation, the evaluator found that the TSS states that:</p>
<p><b>The TSF destroys keys in RAM by performing an overwrite with zeroes.</b></p>
<p><b>The TSF destroys keys stored in non-volatile memory by logically addressing the storage location and performing an overwrite with zeros. Once the overwrite is complete, the file storing the key is deleted. Please see</b> Error! Reference source not found.<b>below for an i dentification of cryptographic keys, storage locations, generation methods, and timing of zeroization.</b></p>
<p>The following table describes the origin, storage and zeroization of keys as relevant to FCS_CKM.4 and FPT_SKP_EXT.1 provided by the TOE.</p>
<table>
<tr><th>Key</th><th>Type</th><th>Origin</th><th>Storage/Protection</th><th>Zeroization</th></tr>
<tr><td>EC Diffie-Hellman Key</td><td>Private ECDH P-256, P-384, or P-521</td><td>TOE generated</td><td>RAM</td><td>Keys are overwritten with zeros when session closes</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>TLS Private Key</td><td>Private ECDSA P-256</td><td>TOE generated</td><td>Restricted Filesystem access</td><td>Zeroize command</td></tr>
<tr><td>TLS Encryption Key</td><td>128-bit or 256-bit AES</td><td>TOE generated</td><td>RAM</td><td>Keys are overwritten with zeros when session closes</td></tr>
<tr><td>TLS Integrity Key</td><td>HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384</td><td>TOE generated</td><td>RAM</td><td>Keys are overwritten with zeros when session closes</td></tr>
</table>
Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

5.2.3.3 FCS_CKM.4 TSS 3

Objective	Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator shall check that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4.
Evaluator Findings	The evaluator examined the section titled **Key storage and zeroization** under **TOE summary and specification** in the Security Target to verify that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4. Upon investigation, the evaluator found that the TSS states that no keys are stored in non-plaintext form. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.4 FCS_CKM.4 TSS 4

Objective	The evaluator shall check that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation section below). Note that reference may be made to the Guidance Documentation for description of the detail of such cases where destruction may be prevented or delayed.
Evaluator Findings	The evaluator examined the section titled **Cryptographic Key Destruction** under **TOE summary and specification** in the Security Target to verify that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement. Upon investigation, the evaluator found that the TSS states that the TOE zeroizes all secrets, keys, and associated values when they are no longer required. Hence no circumstances were found where destruction may be prevented or delayed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.5 FCS_CKM.4 TSS 5

Objective	Where the ST specifies the use of “a value that does not contain any CSP” to overwrite keys, the evaluator examines the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs.
Evaluator Findings	The evaluator verified that ST does not specify the use of ‘a value that does not contain any CSP’ to overwrite keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.6 FCS_CKM.4 Guidance 1

Objective	A TOE may be subject to situations that could prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS (and any other supporting information used). The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.
Evaluator Findings	The evaluator examined the section titled **Zeroization** in the AGD to verify that it identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS. Upon investigation, the evaluator found no items that did not meet conformance to the key destruction requirement. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4 FCS_COP.1/DataEncryption

5.2.4.1 FCS_COP.1/DataEncryption TSS 1

Objective	The evaluator shall examine the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption.
Evaluator Findings	The evaluator examined the **FCS_COP.1/DataEncryption** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the TSS states that: **The TSF performs AES encryption and decryption in CBC and GCM modes with 128 and 256-bit keys for TLS.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.2 FCS_COP.1/DataEncryption Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption.

Evaluator Findings	The evaluator examined the section titled **Log In, Set Admin UI for Login, TLS and Custom ECC Cipher Suite Setand Elliptical Curve Cipher Set** in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the AGD states the claimed cipher suites in Elliptical Curve Cipher and sections Log In and Set Admin UI for Login, TLS and Custom ECC Cipher Suite Set include steps to log in to the TOE and configure custom ECC Cipher Suite. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.3 FCS_COP.1/DataEncryption Test/CAVP 1

Objective	The evaluator shall verify the implementation of encryption supported by the TOE.
Evaluator Findings	CAVP AES Certs: #C2076 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5 FCS_COP.1/SigGen

5.2.5.1 FCS_COP.1/SigGen TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services.
Evaluator Findings	The evaluator examined the **FCS_COP.1/SigGen** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS to ensure it specifies the cryptographic algorithm and key size supported by the TOE for signature services. Upon investigation, the evaluator found that the TSS states that: **The TSF performs RSA 2048 signature verification to verify the integrity and authenticity of updates.** **The TSF performs ECDSA P-256 signature generation and verification as part of TLS.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5.2 FCS_COP.1/SigGen Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services.
Evaluator Findings	The evaluator examined the sections titled **Admin WUI Access** and **Set Admin UI for Login, TLS and Custom ECC Cipher Suite Set** in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services. Upon investigation, the evaluator found that the AGD states steps to configure self-signed certificates. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.2.5.3 FCS_COP.1/SigGen Test/CAVP 1

Objective	The evaluator shall verify the implementation of signature generation and verification supported by the TOE.
Evaluator Findings	CAVP ECDSA&SigVer SigGen (186-4) Certs: #C2076 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6 FCS_COP.1/Hash

5.2.6.1 FCS_COP.1/Hash TSS 1

Objective	The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.
Evaluator Findings	The evaluator examined the **FCS_COP.1/Hash** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS documents the association of the hash function with other TSF cryptographic functions. Upon investigation, the evaluator found that the TSS states that: **The TSF performs SHA-1, SHA-256, SHA-384, and SHA-512 hashing.** **Hashing of are used for the following security functions:** • **NTP – SHA-1** • **Digital Signature generation and verification – SHA-256** • **File Integrity Checking – SHA-256** • **Password Hashing – SHA-512** • **HMAC primitive – SHA-1, SHA-256, SHA-384** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.2 FCS_COP.1/Hash Guidance 1

Objective	The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.
Evaluator Findings	The evaluator examined the section titled **Hash Cryptographic Operation (Hash Algorithm)** in the AGD to verify that it presents any configuration that is required to configure the required hash sizes. Upon investigation, the evaluator found that the AGD states the TOE supports cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384, SHA-512 and message digest sizes 160, 256, 384, 512 bits that meet the following: ISO/IEC 10118-3:2004. The TOE comes preconfigured for these sizes and no additional configuration is required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.3 FCS_COP.1/Hash Test/CAVP 1

Objective	The evaluator shall verify the implementation of hashing supported by the TOE.
Evaluator Findings	CAVP SHA Certs: #C2076 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7 FCS_COP.1/KeyedHash

5.2.7.1 FCS_COP.1/KeyedHash TSS 1

<table>
<tr><td>Objective</td><td>The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function`: key length, hash function used, block size, and output MAC length used.</td></tr>
<tr><td>Evaluator Findings</td><td>The evaluator examined the <b>FCS_COP.1/KeyedHash</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS states that:
<b>The TSF uses the following HMAC algorithms in TLS:</b>
<table>
<tr><th>Algorithm</th><th>Hash Function</th><th>Block Size</th><th>Key Size</th><th>Digest Size</th></tr>
<tr><td>HMAC-SHA-1</td><td>SHA-1</td><td>512 bits</td><td>160 bits</td><td>160 bits</td></tr>
<tr><td>HMAC-SHA-256</td><td>SHA-256</td><td>512 bits</td><td>256 bits</td><td>256 bits</td></tr>
<tr><td>HMAC-SHA-384</td><td>SHA-384</td><td>1024 bits</td><td>384 bits</td><td>384 bits</td></tr>
</table>
Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

5.2.7.2 FCS_COP.1/KeyedHash Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function.
Evaluator Findings	The evaluator examined the section titled **Keyed Hash Cryptographic Operation (Keyed Hash Algorithm)** in the AGD to verify how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function. Upon investigation, the evaluator found that the AGD states that the TOE supports keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and cryptographic key sizes 160-bits, 256-bits, 384-bits, and message digest sizes 160, 256, 384 bits that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2". The TOE comes preconfigured for these sizes and no additional configuration is required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7.3 FCS_COP.1/KeyedHash Test/CAVP 1

Objective	The evaluator shall verify the implementation of MACing supported by the TOE.
Evaluator Findings	CAVP HMAC Certs: #C2076 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8 FCS_RBG_EXT.1

5.2.8.1 FCS_RBG_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value.
Evaluator Findings	The evaluator examined the **FCS_RBG_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value. Upon investigation, the evaluator found that the TSS states that: **The TSF implements an SP 800-90A CTR_DRBG using AES-256. The DRBG is seeded with at least 256-bits of entropy from a third-party hardware entropy source.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8.2 FCS_RBG_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality.
Evaluator Findings	The evaluator examined the section titled **Random Bit Generation** in the AGD to verify that it contains appropriate instructions for configuring the RNG functionality. Upon investigation, the evaluator found that the AGD describes how to configure the TOE in the evaluated configuration by enabling CC mode. Additionally, the evaluator found that the guidance specifically states TOE supports random bit generation using CTR_DRBG and when CC mode is enabled no additional configuration is required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8.3 FCS_RBG_EXT.1.1 Test/CAVP 1

Objective	The evaluator shall verify the implementation of SP 800-90A DRBG supported by the TOE.
Evaluator Findings	CAVP DRBG Certs: #C2076 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3 TSS and Guidance Activities (HTTPS)

5.3.1 FCS_HTTPS_EXT.1

5.3.1.1 FCS_HTTPS_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS and determine that enough detail is provided to explain how the implementation complies with RFC 2818.
Evaluator Findings	The evaluator examined the **FCS_HTTPS_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS provides enough detail to explain how the implementation complies with RFC 2818. Upon investigation, the evaluator found that the TSS states that: **The TSF acts as an HTTPS server to secure administrative connections to the WUI. The TSF implements HTTPS as specified in RFC 2818 using TLS as specified in FCS_TLSS_EXT.1.** **The TOE's HTTPS protocol complies with RFC 2818. The TOE implements all "MUST", "REQUIRED", and "SHOULD" statements from the RFC 2818 that are applicable to a HTTP server. The TOE web GUI operates on an explicit TCP port designed to natively implement TLS. The web server attempts to send closure Alerts prior to closing a connection in accordance with section 2.2.2 of RFC 2818.** The evaluator verified the TCP port number as 443, web server is sending closure alerts, and other applicable "MUST", "REQUIRED", and "SHOULD" statements from the RFC 2818 during FCS_TLSS_EXT.1 testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.2 FCS_HTTPS_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server.
Evaluator Findings	The evaluator examined the sections titled **Log In, Admin WUI Access, Set Admin UI for Login, TLS and Custom ECC Cipher Suite Set** and **Set ECC Ciphers for Self-Signed Certificates and Outbound Connections** in the AGD to verify that it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server. Upon investigation, the evaluator found that the AGD describes the components required to login to HTTPS interface for the TOE, generating a certificate and installing the certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4 TSS and Guidance Activities (NTP)

5.4.1 FCS_NTP_EXT.1

5.4.1.1 FCS_NTP_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure it identifies the version of NTP supported, how it is implemented and what approach the TOE uses to ensure the timestamp it receives from an NTP timeserver (or NTP peer) is from an authenticated source and the integrity of the time has been maintained.

Evaluator Findings	The evaluator examined the **FCS_NTP_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies the version of NTP supported, how it is implemented and what approach the TOE uses to ensure the timestamp it receives from an NTP timeserver (or NTP peer) is from an authenticated source and the integrity of the time has been maintained. Upon investigation, the evaluator found that the TSS states that: **The TSF supports time updates using NTPv4. The TSF authentications updates using an administrator configured symmetric key and SHA-1. The TOE rejects broadcast and multicast time updates. The TOE allows up to 10 NTP time sources to be configured.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.2 FCS_NTP_EXT.1 TSS 2

Objective	The TOE must support at least one of the methods or may use multiple methods, as specified in the SFR element 1.2. The evaluator shall ensure that each method selected in the ST is described in the TSS, including the version of NTP supported in element 1.1, the message digest algorithms used to verify the authenticity of the timestamp and/or the protocols used to ensure integrity of the timestamp.
Evaluator Findings	The evaluator examined the **FCS_NTP_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes each method selected in the ST, including the version of NTP supported in element 1.1, the message digest algorithms used to verify the authenticity of the timestamp and/or the protocols used to ensure integrity of the timestamp. Upon investigation, the evaluator found that the TSS states that **The TSF authentications updates using an administrator configured symmetric key and SHA-1.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.3 FCS_NTP_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to ensure it provides the Security Administrator instructions as how to configure the version of NTP supported, how to configure multiple NTP servers for the TOE's time source and how to configure the TOE to use the method(s) that are selected in the ST.
Evaluator Findings	The evaluator examined the section titled **Configuring NTP Server** in the AGD to verify that it provides the administrator instructions as how to configure the version of NTP supported, how to configure multiple NTP servers for the TOE's time source and how to configure the TOE to use the method(s) that are selected in the ST. Upon investigation, the evaluator found that the AGD states the steps to configure NTP server. The TOE allows up to 10 NTP time sources to be configured. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.4 FCS_NTP_EXT.1.2 Guidance 1

Objective	For each of the secondary selections made in the ST, the evaluator shall examine the guidance document to ensure it instructs the Security Administrator how to configure the

	TOE to use the algorithms that support the authenticity of the timestamp and/or how to configure the TOE to use the protocols that ensure the integrity of the timestamp.
Evaluator Findings	The evaluator examined the section titled **Configuring NTP Server** in the AGD to verify that, for each of the secondary selections made in the ST, it instructs the administrator how to configure the TOE to use the algorithms that support the authenticity of the timestamp and/or how to configure the TOE to use the protocols that ensure the integrity of the timestamp. Upon investigation, the evaluator found that the AGD describes detailed instructions how to configure the TOE to use the algorithms that support the authenticity of the timestamp and how to configure the TOE to use the protocols that ensure the integrity of the timestamp. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.5 FCS_NTP_EXT.1.3 Guidance 1

Objective	The evaluator shall examine the guidance documentation to ensure it provides the Security Administrator instructions as how to configure the TOE to not accept broadcast and multicast NTP packets that would result in the timestamp being updated.
Evaluator Findings	The evaluator examined the section titled **Configuring NTP Server** in the AGD to verify that it provides instructions as how to configure the TOE to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. Upon investigation, the evaluator found that the AGD states that **the TOE rejects broadcast and multicast time updates.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (TLS)

5.5.1 FCS_TLSC_EXT.1

5.5.1.1 FCS_TLSC_EXT.1.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified include those listed for this component.
Evaluator Findings	The evaluator examined the **FCS_TLSC_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS specifies the ciphersuites supported and that the ciphersuites specified include those listed for this component. Upon investigation, the evaluator found that the TSS states that: **The TSF is a TLS client for securing communications with Syslog and LDAP servers. The TSF supports TLSv1.2 and TLSv1.1 with the following ciphersuites:** • **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA** • **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA** • **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256** • **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384** • **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** • **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.2 FCS_TLSC_EXT.1.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS.
Evaluator Findings	The evaluator examined the section titled **Set Admin UI for Login, TLS and Custom ECC Cipher Suite Set** in the AGD to verify that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD describes the instructions on configuring TLS on TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.3 FCS_TLSC_EXT.1.2 TSS 1

Objective	The evaluator shall ensure that the TSS describes the client's method of establishing all reference identifiers from the administrator/application configured reference identifier, including which types of reference identifiers are supported (e.g., application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported.
Evaluator Findings	The evaluator examined the **FCS_TLSC_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the client's method of establishing all reference identifiers from the administrator/application-configured reference identifier, including which types of reference identifiers are supported; whether IP addresses and wildcards are supported. Upon investigation, the evaluator found that the TSS states that: **The TSF supports the following identifier types:** • **DNS name in the SAN or CN. Wildcards are supported in the left-most position.** • **IPv4 address in the SAN or CN.** **The TSF only checks the identifier in the CN if the SAN extension is not present. The TSF does not support SRV or URI identifiers. The reference identifier for external IT devices are configured by the administrator using the available administrative commands in the CLI. The reference identifiers must be an IPv4 address or a hostname.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.4 FCS_TLSC_EXT.1.2 TSS 2

Objective	If IP addresses are supported in the CN as reference identifiers, the evaluator shall ensure that the TSS describes the TOE's conversion of the text representation of the IP address in the CN to a binary representation of the IP address in network byte order. The evaluator shall also ensure that the TSS describes whether canonical format (RFC 5952 for IPv6, RFC 3986 for IPv4) is enforced.
Evaluator Findings	The evaluator examined the **FCS_TLSC_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that, if IP addresses are supported in the CN as reference identifiers, the TSS describes the TOE's conversion of the text representation of the

	IP address in the CN to a binary representation of the IP address in network byte order and whether canonical format is enforced. Upon investigation, the evaluator found that the TSS states that **When the reference identifier is an IP address, the TOE converts the IP address to a binary representation in network byte order. IPv4 addresses are converted directly from decimal to binary with period "." serving as the delineator. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name extension. If there is not an exact binary match, then the verification fails. If the SAN entry is missing, the TOE will compare the IPv4 address against the Common Name (CN). If the IPv4 address in CN is not an exact binary match, then the verification fails. For IPv4 address in SAN or CN matching, the IPv4 address must be an exact binary match.** **The TLS channel is terminated if verification fails.** **SAN is prioritized over CN. The TOE does not enforce canonical format.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.5 FCS_TLSC_EXT.1.2 Guidance 1

Objective	The evaluator shall ensure that the operational guidance describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). If the identifier scheme implemented by the TOE includes support for IP addresses, the evaluator shall ensure that the operational guidance provides a set of warnings and/or CA policy recommendations that would result in secure TOE use.
Evaluator Findings	The evaluator examined the section titled **Secure Remote Logging** and **Reference Identifiers** in the AGD to verify that it describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not, includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s), and provides a set of warnings and/or CA policy recommendations that would result in secure TOE use. Upon investigation, the evaluator found that the AGD provides a description of how reference identifiers are used for TLS. This description includes the supported identifiers, SAN support, CN support, wildcard support, and how to configure reference identifiers on the TOE. • When the reference identifier is a hostname, the TOE compares the hostname against all the DNS Name entries in the Subject Alternative Name (SAN) extension. If the hostname does not match any of the DNS Name entries, then the verification fails. If the certificate does not contain any DNS Name entries in SAN, the TOE will compare the hostname against the Common Name (CN). If the hostname does not match the CN, then the verification fails. For both DNS Name and CN matching, the hostname must be an exact match or wildcard match. In the case of a wildcard match, the wildcard must be the left-most component, wildcard matches a single component, and there are at least two non-wildcard components. • When the reference identifier is an IP address, the TOE converts the IP address to a binary representation in network byte order. IPv4 addresses are converted directly from decimal to binary with period "." serving as the delineator. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name extension. If there is not an exact binary match, then the verification fails. If the SAN entry is missing,

	the TOE will compare the IPv4 address against the Common Name (CN). If the IPv4 address in CN is not an exact binary match, then the verification fails. For IPv4 address in SAN or CN matching, the IPv4 address must be an exact binary match. Note: SAN is prioritized over CN. Warning: The above-mentioned reference identifier matching rules should be taken into consideration while connecting to peers or IT entities using certificates that have DNS or IP Address. • The TLS channel is terminated if verification fails. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.6 FCS_TLSC_EXT.1.4 TSS 1

Objective	The evaluator shall verify that TSS describes the Supported Elliptic Curves/Supported Groups Extension and whether the required behavior is performed by default or may be configured.
Evaluator Findings	The evaluator examined the **FCS_TLSC_EXT.1** entry in section titled **Cryptographic Support (FCS)** in the Security Target to verify that the TSS describes the Supported Elliptic Curves Extension and whether the required behavior is performed by default or may be configured. Upon investigation, the evaluator found that the TSS states that **the TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: secp256r1, secp384r1, and secp521r1.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.7 FCS_TLSC_EXT.1.4 Guidance 1

Objective	If the TSS indicates that the Supported Elliptic Curves/Supported Groups Extension must be configured to meet the requirement, the evaluator shall verify that AGD guidance includes configuration of the Supported Elliptic Curves/Supported Groups Extension.
Evaluator Findings	The evaluator examined the **FCS_TLSC_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to check whether the Supported Elliptic Curves Extension must be configured or not. Upon investigation, the evaluator found that the ST states that The TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by **default** with support for the following NIST curves: secp256r1, secp384r1, and secp521r1. Therefore, no configuration is required and hence the AGD is not required to provide any configuration guidance. The evaluator also verified the Section titled **SAN Extension** in the AGD and it states that The TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by **default** with support for the following NIST curves: secp256r1, secp384r1, and secp521r1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2 FCS_TLSS_EXT.1

5.5.2.1 FCS_TLSS_EXT.1.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS specifies the ciphersuites supported and that the ciphersuites specified are identical to those listed for this component. Upon investigation, the evaluator found that the TSS states that: **The TSF is an HTTPS/TLS server for providing the WUI trusted channel to remote administrators. The TSF supports TLSv1.2 and TLSv1.1 with the following ciphersuites:** • **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA** • **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA** • **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256** • **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384** • **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** • **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.2 FCS_TLSS_EXT.1.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	The evaluator examined the section titled **Set Admin UI for Login, TLS and Custom ECC Cipher Suite Set** in the AGD to verify that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD describes the instructions on configuring TLS on TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.3 FCS_TLSS_EXT.1.2 TSS 1

Objective	The evaluator shall verify that the TSS contains a description of how the TOE technically prevents the use of old SSL and TLS versions.
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS contains a description of the denial of old SSL and TLS versions. Upon investigation, the evaluator found that the TSS states that: **The TSF rejects the connection if the client attempts to establish a connection using an older version of TLS or SSL.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.4 FCS_TLSS_EXT.1.2 Guidance 1

Objective	The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.
Evaluator Findings	The evaluator examined the section titled **Set Admin UI for Login, TLS and Custom ECC Cipher Suite Set** in the AGD to verify that it contains any configuration necessary to meet the requirement must be contained in the AGD guidance. Upon investigation, the evaluator found that the AGD states that the AGD describes the instructions on configuring TLS on TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.5 FCS_TLSS_EXT.1.3 TSS 1

Objective	If using ECDHE and/or DHE ciphers, the evaluator shall verify that the TSS lists all EC Diffie-Hellman curves and/or Diffie-Hellman groups used in the key establishment by the TOE when acting as a TLS Server. For example, if the TOE supports TLS_DHE_RSA_WITH_AES_128_CBC_SHA cipher and Diffie-Hellman parameters with size 2048 bits, then list Diffie-Hellman Group 14. **[TD0635 applied]**
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that, if using ECDHE or DHE ciphers, the TSS describes the key agreement parameters of the server Key Exchange message. Upon investigation, the evaluator found that the TSS states that: **The TSF will perform ECDHE key establishment using secp256r1, secp384r1, and secp521r1. If the client did not propose one of these curves, the connection fails.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.6 FCS_TLSS_EXT.1.3 Guidance 1

Objective	The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.
Evaluator Findings	The evaluator examined the section titled **Set ECC Ciphers for Self-Signed Certificates and Outbound Connections** in the AGD to verify that it contains any configuration necessary to meet the requirement. Upon investigation, the evaluator found that the AGD states that **no configuration is required other than enabling CC mode.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.7 FCS_TLSS_EXT.1.4 TSS 1

Objective	The evaluator shall verify that the TSS describes if session resumption based on session IDs is supported (RFC 4346 and/or RFC 5246) and/or if session resumption based on session tickets is supported (RFC 5077).
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target. Upon investigation, the evaluator found that the TSS states that:

	The TSF does not support session resumption or session tickets. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.8 FCS_TLSS_EXT.1.4 TSS 2

Objective	If session tickets are supported, the evaluator shall verify that the TSS describes that the session tickets are encrypted using symmetric algorithms consistent with FCS_COP.1/DataEncryption. The evaluator shall verify that the TSS identifies the key lengths and algorithms used to protect session tickets.
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target. Upon investigation, the evaluator found that the TSS states that **The TSF does not support session resumption or session tickets.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.9 FCS_TLSS_EXT.1.4 TSS 3

Objective	If session tickets are supported, the evaluator shall verify that the TSS describes that session tickets adhere to the structural format provided in section 4 of RFC 5077 and if not, a justification shall be given of the actual session ticket format.
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target. Upon investigation, the evaluator found that the TSS states that **The TSF does not support session resumption or session tickets.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.10 FCS_TLSS_EXT.1.4 TSS 4 **[TD0569]**

Objective	If the TOE claims a (D)TLS server capable of session resumption (as a single context, or across multiple contexts), the evaluator verifies that the TSS describes how session resumption operates (i.e., what would trigger a full handshake, e.g., checking session status, checking Session ID, etc.). If multiple contexts are used the TSS describes how session resumption is coordinated across those contexts. In case session establishment and session resumption are always using a separate context, the TSS shall describe how the contexts interact with respect to session resumption (in particular regarding the session ID). It is acceptable for sessions established in one context to be resumable in another context.
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target and determined that the TOE does not claim a (D)TLS server capable of session resumption. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6 TSS and Guidance Activities (Identification and Authentication)

5.6.1 FIA_AFL.1

5.6.1.1 FIA_AFL.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability.
Evaluator Findings	The evaluator examined the **FIA_AFL.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked; the method by which the remote administrator is prevented from successfully logging on to the TOE; and the actions necessary to restore this ability. Upon investigation, the evaluator found that the TSS states that **The TSF blocks remote authentication attempts after a configurable number of failed attempts (both password and cert-based attempts). The security administrator can configure the threshold to be from 1 through 999. Once an account is locked, the account must be unlocked using the "bal" account at the local console. The administration of the TSF is always possible, because the TSF never locks the local console.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.2 FIA_AFL.1 TSS 2

Objective	The evaluator shall examine the TSS to confirm that the TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily (e.g., by providing local logon which is not subject to blocking).
Evaluator Findings	The evaluator examined the **FIA_AFL.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available. Upon investigation, the evaluator found that the TSS states that: **Once an account is locked, the account must be unlocked using the "bal" account at the local console (applicable only to web GUI). The administration of the TSF is always possible, because the TSF never locks the local console.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.3 FIA_AFL.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to ensure that instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.

Evaluator Findings	The evaluator examined the section titled **Failed Login Attempts** and **Idle Session Timeout** in the AGD to verify that it provides instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented), and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). Upon investigation, the evaluator found that the AGD states the steps to configure the number of times that a user can fail to login correctly and the length of time (in seconds) a user can be idle (no activity recorded) before they are logged out of the session is defined. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.4 FIA_AFL.1 Guidance 2

Objective	The evaluator shall examine the guidance documentation to confirm that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1.
Evaluator Findings	The evaluator examined the section titled **Log In** and **Set ECC Ciphers for Self-Signed Certificates and Outbound Connections** in the AGD to verify that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1. Upon investigation, the evaluator found that a section **Log In** in AGD states **that the 'bal' administrative login, and the password you specified during installation. And section Set ECC Ciphers for Self-Signed Certificates and Outbound Connections** in the AGD states that **Factory reset does not change the "bal" password.** Based on these findings, this assurance activity is considered satisfied.

5.6.2 FIA_PMG_EXT.1

5.6.2.1 FIA_PMG_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords.
Evaluator Findings	The evaluator examined the **FIA_PMG_EXT.1.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords. Upon investigation, the evaluator found that the TSS states that: **The TSF allows administrators passwords to be composed of any printable ASCII character (i.e., 0x20-0x7E inclusive).** **The TSF allows the security administrator to configure the minimum password length to be 8-16 characters.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2.2 FIA_PMG_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that it: a) identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.
Evaluator Findings	The evaluator examined the section titled **Set Minimum Password Length** in the AGD to verify that it identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords and provides instructions on setting the minimum password length and describes the valid minimum password lengths supported. Upon investigation, the evaluator found that the AGD states the steps to configure minimum password length and all characters which includes combination of lowercase, uppercase letters, numbers, and special characters are allowed while setting the password. For strong passwords the Minimum Password Length should meet. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3 FIA_UIA_EXT.1

5.6.3.1 FIA_UIA_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a "successful logon".
Evaluator Findings	The evaluator examined the **FIA_UIA_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the logon process for each logon method supported for the product. Upon investigation, the evaluator found that the TSS states that: **Authentication is based on username/password for the web interface and local console. The TOE does not expose any interface, through any access method prior to successful login.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.2 FIA_UIA_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to determine that it describes which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration.
Evaluator Findings	The evaluator examined the **FIA_UIA_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes which actions are allowed before user identification and authentication. Upon investigation, the evaluator found that the TSS states that: **Prior to authentication, the TSF only allows users to display the warning banner and automatically generate keys on a new system.**

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.3 FIA_UIA_EXT.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the guidance documentation provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the guidance documentation provides sufficient instruction on limiting the allowed services.
Evaluator Findings	The evaluator examined the section titled **Log In, Set the GUI Banner and Set the CLI Banner** in AGD to verify that it describes any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in. Upon investigation, the evaluator found that the AGD states that regardless of method of administering the TOE, the user is presented with a banner and then with an authentication prompt. At the authentication prompt the username of the administrator and credential (password) must be presented. Administration is available only after the correct username/credential combination is presented. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4 FIA_UAU.7

5.6.4.1 FIA_UAU.7 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed.
Evaluator Findings	The evaluator examined the entire AGD and verified that no preparatory steps are required to ensure that authentication data is not revealed while entering the credentials. It was found during testing that the TOE does not provide any feedback while entering the password at both the directly connected and remote login prompt. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5 FIA_X509_EXT.1/Rev

5.6.5.1 FIA_X509_EXT.1/Rev TSS 1

Objective	The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e., where the ST is therefore claiming that they are trivially satisfied). It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).

Evaluator Findings	The evaluator examined the **FIA_X509_EXT.1/Rev** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). Upon investigation, the evaluator found that the TSS states that: **The TOE performs X.509 certificate validation at the following points:** • **TOE TLS client authentication of server X.509 certificates.** • **TOE TLS server authentication of client X.509 certificates.** • **When certificates are loaded into the TOE, such as when importing Cas and certificate responses.** **In all scenarios, certificates are checked for several validation characteristics:** • **If the certificate 'notAfter' date is in the past, then this is an expired certificate which is considered invalid.** • **The certificate chain must terminate with a certificate designated as a trust anchor on the TOE.** • **All certificates not designated as trust anchors must not be revoked, as indicated by an OCSP status check.** • **All trust anchor and intermediate certificates must contain the basicConstraints extension and have the CA flag set to TRUE.** • **Server certificates consumed by the TOE TLS client must have a 'serverAuthentication' extendedKeyUsage purpose.** • **Client certificates consumed by the TOE TLS server must have a 'clientAuthentication' extendedKeyUsage purpose.** **Certificates used to sign OCSP responses must have the OCSP signing purpose in the extendedKeyUsage extension.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.2 FIA_X509_EXT.1/Rev TSS 2

Objective	The TSS shall describe when revocation checking is performed and on what certificates. If the revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented, any differences must be summarized in the TSS section and explained in the Guidance.
Evaluator Findings	The evaluator examined the **FIA_X509_EXT.1/Rev** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes when revocation checking is performed and on what certificates. Upon investigation, the evaluator found that the TSS states that **All certificates not designated as trust anchors must not be revoked, as indicated by an OCSP status check**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.3 FIA_X509_EXT.1/Rev Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e., where the ST is therefore claiming that they are trivially satisfied) and describes how certificate revocation checking is performed and on which certificate.
Evaluator Findings	The evaluator examined the section titled **Set Admin UI for Login, TLS and Custom ECC Cipher Suite Set** and section **Set ECC Ciphers for Self-Signed Certificates and Outbound Connections** in the AGD to verify that it contains describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE and describes how certificate revocation checking is performed and on which certificate. Upon investigation, the evaluator found that the AGD states that how certificate validation takes place. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6 FIA_X509_EXT.2

5.6.6.1 FIA_X509_EXT.2 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use.
Evaluator Findings	The evaluator examined the **FIA_X509_EXT.2** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how the TOE chooses which certificates to use. Upon investigation, the evaluator found that the TSS states that: **As a TLS Client, the TOE uses OCSP to determine whether the certificate is revoked or not. When the TSF does not receive a response from an OCSP server, by default, the TSF rejects the certificate. The administrator can configure the TSF to accept certificates when an OCSP response is not received.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.2 FIA_X509_EXT.2 TSS 2

Objective	The evaluator shall examine the TSS to confirm that it describes the behavior of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	The evaluator examined the **FIA_X509_EXT.2.2** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the behavior of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. Upon investigation, the evaluator found that the TSS states that: **The administrator can configure the TSF to accept certificates when an OCSP response is not received.**

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.3 FIA_X509_EXT.2 Guidance 1

Objective	The evaluator shall check the administrative guidance to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	The evaluator examined the section titled **Generate CSR (Certificate Signing Request), Set ECC Ciphers for Self-Signed Certificates and Outbound Connections, Enable OCSP Checking and Stapling, Intermediate Certificate, Lockdown Admin UI logon to Certificate Only with OCSP validation** in the AGD to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the AGD provides instructions and warnings for the configuring the operating environment so that the TOE can use the certificates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.4 FIA_X509_EXT.2 Guidance 2

Objective	If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	The evaluator examined the section titled **Enable OCSP Checking** in the AGD to verify that, if the requirement that the administrator is able to specify the default action, the guidance documentation contains instructions on how this configuration action is performed. Upon investigation, the evaluator found that the AGD states that **enabling the allow access on server failure option treats an OCSP server connection failure or timeout as if the OCSP server has returned a valid response.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.5 FIA_X509_EXT.2 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes the configuration required in the operating environment so the TOE can use the certificates. The guidance documentation shall also include any required configuration on the TOE to use the certificates. The guidance document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.
Evaluator Findings	The evaluator examined the section titled **Generate CSR (Certificate Signing Request) and Intermediate Certificate** in the AGD. Upon investigation, the evaluator found that the AGD describes how to use certificates and steps to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.7 FIA_X509_EXT.3

5.6.7.1 FIA_X509_EXT.3 TSS 1

Objective	If the ST author selects "device-specific information", the evaluator shall verify that the TSS contains a description of the device-specific fields used in certificate requests.
Evaluator Findings	The evaluator examined the **FIA_X509_EXT.3** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS contains a description of the device-specific fields used in certificate requests. Upon investigation, the evaluator found that the TSS states that: **The TSF is capable of generating certificate signing request that contain the public key, device specific information (e.g., email address, requested SAN name), Common Name, Organization, Organizational Unit, Country** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.7.2 FIA_X509_EXT.3 Guidance 1

Objective	The evaluator shall check to ensure that the guidance documentation contains instructions on requesting certificates from a CA, including generation of a Certificate Request. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the evaluator shall ensure that this guidance includes instructions for establishing these fields before creating the Certification Request.
Evaluator Findings	The evaluator examined the section titled **Generate CSR (Certificate Signing Request)** in the AGD to verify that it contains instructions on requesting certificates from a CA, including generation of a Certification Request. Upon investigation, the evaluator found that the AGD includes instructions for **device specific information (e.g. email address, requested SAN name), Common Name, Organization, Organizational Unit, Country**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7 TSS and Guidance Activities (Security Management)

5.7.1 FMT_MOF.1/ManualUpdate

5.7.1.1 FMT_MOF.1/ManualUpdate Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary steps to perform manual update are described. The guidance documentation shall also provide warnings regarding functions that may cease to operate during the update (if applicable).
Evaluator Findings	The evaluator examined the section titled **Installing an Update Image** in the AGD to verify that it describes any necessary steps to perform manual update. Upon investigation, the evaluator found that the AGD states that the AGD describes the steps to follow while performing the update. The evaluator examined the section titled **Installing an Update Image** in the AGD to verify that it provides warnings regarding functions that may cease to operate during the update (if

	applicable). Upon investigation, the evaluator found that the AGD also gives warnings if corrupt or invalid verification file is uploaded during the update. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2 FMT_MTD.1/CoreData

5.7.2.1 FMT_MTD.1/CoreData TSS 1

Objective	The evaluator shall examine the TSS to determine that, for each administrative function identified in the guidance documentation; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.
Evaluator Findings	The evaluator examined **FMT_MTD.1/CoreData** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users. Upon investigation, the evaluator found that the TSS states that: **The TSF displays a warning banner prior to user authentication. There are no administrative functions available for unauthorized users. All administrators must be authenticated and authorized to perform any activity that can alter TSF data.** **The TSF restricts the ability to manage TSF data to security administrators.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2.2 FMT_MTD.1/CoreData TSS 2

Objective	If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator shall examine the TSS to determine that it contains sufficient information to describe how the ability to manage the TOE's trust store is restricted.
Evaluator Findings	The evaluator examined the **FMT_MTD.1/CoreData** entry in section titled **TOE Summary Specification** in the Security Target to verify that, if the TOE supports handling of X.509v3 certificates and implements a trust store, the TSS contains sufficient information to describe how the ability to manage the TOE's trust store is restricted. Upon investigation, the evaluator found that the TSS states that: **The TSF restricts the ability to manage TSF data to security administrators.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2.3 FMT_MTD.1/CoreData Guidance 1

Objective	The evaluator shall review the guidance documentation to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.

Evaluator Findings	The evaluator examined the entire AGD to verify that it identifies each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP. Upon investigation, the evaluator found that the following sections in the AGD describes the configuration available for each of the TSF-data manipulating functions available on the TOE, which is consistent with the requirements of the cPP identified in the ST. **'User Creation'** **'Set Minimum Password Length'** **'Intermediate Certificate'** **'Generate CSR (Certificate Signing Request)'** **'Logging out'** **'Log in'** **'Setting Date/Time'** **'Setup Admin UI Access via LDAP'** **'Secure Remote Logging'** **'Idle Session Timeout'** **'Failed Login Attempts'** **'Set the GUI Banner'** **'Set the CLI Banner'** **'Configuring NTP server'** **The section entitled "CC Configuration Process" covers each of the TSF-data manipulating functions available on the TOE and explains that when administrators log in with role-based credentials, their access is limited to commands they have privileges and permissions to use based on the Common Criteria standards. No management functionality is available prior to successful identification and authentication of the users.** **Network management communication paths are protected against modification and disclosure by TLS.** **The set of subsections within the section entitled "Intermediate Certificate" and "Generate CSR (Certificate Signing Request)" describe administrative actions that administrators can perform to manage certificates and generate certificate-signing-request respectively.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2.4 FMT_MTD.1/CoreData Guidance 2

Objective	If the TOE supports handling of X.509v3 certificates and provides a trust store, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. If the TOE supports loading of CA certificates, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to securely load CA certificates into the trust store. The evaluator shall also review the guidance documentation to determine that it explains how to designate a CA certificate a trust anchor.

Evaluator Findings	The evaluator examined the section titled **Log In** in the AGD to verify that, if the TOE supports handling of X.509v3 certificates and provides a trust store, it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. Upon investigation, the evaluator found that the AGD states that only the administrator or the user with all permissions can configure and maintain trust store. The evaluator examined the section titled **Set ECC Ciphers for Self-Signed Certificates and Outbound Connections** in the AGD to verify that, if the TOE supports loading of CA certificates, it provides sufficient information for the administrator to securely load CA certificates into the trust store and that it explains how to designate a CA certificate a trust anchor. Upon investigation, the evaluator found that the AGD states steps to upload EC and RSA signatures self-signed certificates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3 FMT_MTD.1/CryptoKeys

5.7.3.1 FMT_MTD.1/CryptoKeys TSS 1

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g., generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	The evaluator examined the **FMT_MTD.1/CryptoKeys** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g., generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the TSS states that: **The TSF allows the security administrator to generate cryptographic keys associated with the TSF's self-signed web server certificate or Certificate Signing Requests.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.2 FMT_MTD.1/CryptoKeys Guidance 1

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	The evaluator examined the section titled **'ECC Ciphers for Self-Signed Certificates and Outbound Connections'** in the AGD to verify that it lists the keys the Security Administrator is able to manage to include the options available (e.g., generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the AGD states that **the AGD provides instructions for the configuring the usage of certificates**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4 FMT_SMF.1

5.7.4.1 FMT_SMF.1 TSS 1

Objective	The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface). The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface.
Evaluator Findings	The evaluator examined the **FMT_SMF.1** entry in section titled **TOE Summary Specification** in the TSS to verify that it details which security management functions are available through which interface(s). The evaluator examined the following sections in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator mentioned the respective sections in AGD for the points stated in the TSS as below: The TSF supports local (Console) and remote (WUI) administrative interfaces. **The following management functions are available at the Console:** • **Manage cryptographic keys** **The following management functions are available via the WUI:** • **Configure the access banner** • **Configure the session inactivity timer** • **Initiate manual updates** • **Managed cryptographic keys** • **Configure TLS versions and ciphersuites** • **Set the time** • **Configure NTP** • **Configure the reference identifier for the Syslog and LDAP servers** • **Manage the X.509 certificate trust store** • **Import X.509 certificates into the trust store.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.2 FMT_SMF.1 Guidance 1

Objective	The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local.
Evaluator Findings	The evaluator examined the section titled **Using CLI** in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD describes the login process for Using CLI. The evaluator examined the section titled **Using CLI** in the AGD to verify that it includes appropriate warnings for the administrator to ensure the interface is local. Upon investigation, the evaluator found that the AGD states audit logs are generated for each session. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.7.5 FMT_SMR.2

5.7.5.1 FMT_SMR.2 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE.
Evaluator Findings	The evaluator examined the section titled **FMT_SMR.2** in the TSS and the section titled **Log In** in the AGD to verify that the TOE supported roles and any restrictions of the roles involving administration of the TOE. Upon investigation, the evaluator found that the ST states that **The TSF supports a bal account (superuser) and administrator accounts. Both account types belong to the Security Administrator role.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.2 FMT_SMR.2 Guidance 1

Objective	The evaluator shall review the guidance documentation to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.
Evaluator Findings	The evaluator examined the section titled **Log In** and **Using CLI** in the AGD to verify that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. Upon investigation, the evaluator found that the AGD describes the steps and instructions for local and remote monitoring. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8 TSS and Guidance Activities (Protection of the TSF)

5.8.1 FPT_APW_EXT.1

5.8.1.1 FPT_APW_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored. The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.
Evaluator Findings	The evaluator examined the **FPT_APW_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS details all authentication data that are subject to this requirement and the method used to obscure the plaintext password data when stored. The evaluator also examined that the TSS details that passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that **The TSF stores administrative passwords protected by a SHA-512 hash.** Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.8.2 FPT_SKP_EXT.1

5.8.2.1 FPT_SKP_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how any preshared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.
Evaluator Findings	The evaluator examined the **FPT_SKP_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that: **The TSF prevents reading symmetric and private keys. The private TLS certificate keys are protected through UI restrictions that prevent the security administrators from reading the keys. All other symmetric and private keys are only held in RAM and can only be accessed by the processes performing TLS. The TSF does not utilize pre-shared keys.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3 FPT_STM_EXT.1

5.8.3.1 FPT_STM_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time, and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. If “obtain time from the underlying virtualization system” is selected, the evaluator shall examine the TSS to ensure that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay. **[TD0632 applied]**
Evaluator Findings	The evaluator examined the **FPT_STM_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists each security function that makes use of time and provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. Upon investigation, the evaluator found that the TSS states that: **The TSF maintains the date and time using the clock provided by the underlying hardware. This date and time are used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time can be manually updated by a Security Administrator or automatically updated using NTP synchronization.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.2 FPT_STM_EXT.1 Guidance 1

Objective	The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.
Evaluator Findings	The evaluator examined the sections titled **Setting Date/Time** and **Configuring NTP Server** in the AGD to verify that it instructs the administrator how to set the time. Upon investigation, the evaluator found that the AGD describes steps for how to use NTP server and how to set date and time. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4 FPT_TST_EXT.1.1

5.8.4.1 FPT_TST_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.
Evaluator Findings	The evaluator examined the **FPT_TST_EXT.1.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS details the self-tests that are run by the TSF on start-up. Upon investigation, the evaluator found that the TSS states that: **The TSF performs the following tests at power-up:** • **File systems checks** **During boot up the TSF checks file system by verifying the metadata and that it is mounted correctly** • **SHA-256 Software integrity checks** **The TSF generates a SHA-256 has of the firmware image and compares it with the stored value** • **Cryptographic algorithm known answer tests** **For each cryptographic algorithm, the TSF performs a sample cryptographic operation using know values and compares the output with the expected value** • **Cryptographic algorithm pairwise constancy test** **For each cryptographic algorithm with a key-pair, the TSF performs a sample operation using know value and compares the output with the corresponding key-pair** • **Health test of the noise source** **This is a continuous health-test that checks the number of occurrences of 6 different bit patterns in each 256-bit output from the noise source. It checks if any of the pattern counts are outside of predetermined thresholds. If more than 128 of the most recent 256 256-bit samples fails, the Entropy Source cease to output data**

	The evaluator examined the **FPT_TST_EXT.1.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. Upon investigation, the evaluator found that the TSS states that: **If any of the tests fail, the TSF disables the affected functionality or halts. The TSF will boot with cryptographic service disabled if the known answer tests, pairwise consistency test, or noise source health test fail.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.2 FPT_TST_EXT.1.1 Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.
Evaluator Findings	The evaluator examined the section titled **Start-up and Self-Test** in the AGD to verify that it describes the possible errors that may result from such tests, and actions the administrator should take in response. Upon investigation, the evaluator found that the AGD states that If any of the tests fail, the TSF disables the affected functionality or halts. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5 FPT_TUD_EXT.1

5.8.5.1 FPT_TUD_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describe how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active. The evaluator shall verify this description.
Evaluator Findings	The evaluator examined the **FPT_TUD_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how to query the currently active version. Upon investigation, the evaluator found that the TSS states that: **The TSF allows the Security Administrator to query the currently running version of software. The TSF also allows the Security Administrator to initiate software updates.** The evaluator examined the **FPT_TUD_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS, if a trusted update can be installed on the TOE with a delayed activation, describes how and when the inactive version becomes active. Upon investigation, the evaluator found that the trusted update on TOE with a delayed activation not selected in ST. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.2 FPT_TUD_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system firmware and software (for simplicity the term 'software' will be used in the following although the requirements apply to firmware and software). The evaluator shall

	verify that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS shall detail this mechanism instead of the digital signature verification mechanism. The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.
Evaluator Findings	The evaluator examined the **FPT_TUD_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes all TSF software update mechanisms for updating the system software, includes a digital signature verification of the software before installation and that installation fails if the verification fails. Upon investigation, the evaluator found that the TSS states that: **The TSF allows the Security Administrator to query the currently running version of software. The TSF allows the Security Administrator to query the currently running version of software. Prior to installing an update, the TSF verifies an RSA 2048 signature on the update to ensure the update is authentic.** The evaluator examined the **FPT_TUD_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification. Upon investigation, the evaluator found that the TSS states that **Prior to installing an update, the TSF verifies an RSA 2048 signature on the update to ensure the update is authentic.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.3 FPT_TUD_EXT.1 TSS 3

Objective	If the options ‘support automatic checking for updates’ or ‘support automatic updates’ are chosen from the selection in FPT_TUD_EXT.1.2, the evaluator shall verify that the TSS explains what actions are involved in automatic checking or automatic updating by the TOE, respectively.
Evaluator Findings	The evaluator examined the **FPT_TUD_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS, if the options ‘support automatic checking for updates’ or ‘support automatic updates’ are chosen, explains what actions are involved in automatic checking or automatic updating by the TOE. Upon investigation, the evaluator found that the TSS states that support automatic checking for updates’ or ‘support automatic updates’ not chosen in ST. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.4 FPT_TUD_EXT.1 Guidance 1

Objective	The evaluator shall verify that the guidance documentation describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the guidance documentation needs to describe how to query the loaded but inactive version.
Evaluator Findings	The evaluator examined the section titled **Installing an Update Image** in the AGD to verify that it describes how to query the currently active version and, if a trusted update can be installed on the TOE with a delayed activation, the loaded but inactive version. Upon investigation, the evaluator found that the AGD states that **the AGD includes the commands required to show the software version**. **On the Home page of the TOE the current version is seen.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.5 FPT_TUD_EXT.1 Guidance 2

Objective	The evaluator shall verify that the guidance documentation describes how the verification of the authenticity of the update is performed (digital signature verification or verification of published hash). The description shall include the procedures for successful and unsuccessful verification. The description shall correspond to the description in the TSS.
Evaluator Findings	The evaluator examined the section titled **Installing an Update Image** in the AGD to verify that it describes how the verification of the authenticity of the update is performed. Upon investigation, the evaluator found that the AGD states that **After the system validates the image, you'll be asked to confirm the installation to continue.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.6 FPT_TUD_EXT.1 Guidance 3

Objective	If a published hash is used to protect the trusted update mechanism, the evaluator shall verify that the guidance documentation describes how the Security Administrator can obtain authentic published hash values for the updates.
Evaluator Findings	The evaluator examined the Security Target & AGD and verified that published hash is not used to protect the trusted update mechanism. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.7 FPT_TUD_EXT.1 Guidance 4

Objective	If this was information was not provided in the TSS: If the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, the evaluator shall verify that the Guidance Documentation contains a description of how the certificates are contained on the device. The evaluator also ensures that the Guidance Documentation describes how the certificates are installed/updated/selected, if necessary.

Evaluator Findings	The evaluator examined the Security Target & AGD and verified that a certificate-based mechanism is not used for software update digital signature verification. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9 TSS and Guidance Activities (TOE Access)

5.9.1 FTA_SSL_EXT.1

5.9.1.1 FTA_SSL_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details whether local administrative session locking, or termination is supported and the related inactivity time period settings.
Evaluator Findings	The evaluator examined the **FTA_SSL_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies whether local administrative session locking, or termination is supported and the related inactivity time period settings. Upon investigation, the evaluator found that the TSS states that: **The TSF terminates local sessions after 1-1440 minutes of inactivity.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.1.2 FTA_SSL_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states whether local administrative session locking, or termination is supported and instructions for configuring the inactivity time period.
Evaluator Findings	The evaluator examined the section titled **Idle Session Timeout** in the AGD to verify that it states whether local administrative session locking, or termination is supported and instructions for configuring the inactivity time period. Upon investigation, the evaluator found that the AGD states that sessions terminate after passing the configured inactivity period and that this is applicable to both local and remote sessions. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2 FTA_SSL.3

5.9.2.1 FTA_SSL.3 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the administrative remote session termination and the related inactivity time period.
Evaluator Findings	The evaluator examined the **FTA_SSL.3** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies administrative remote session termination and the related inactivity time period. Upon investigation, the evaluator found that the TSS states that: **The TSF terminates remote sessions after 60-86400 seconds of inactivity.** Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.9.2.2 FTA_SSL.3 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation includes instructions for configuring the inactivity time period for remote administrative session termination.
Evaluator Findings	The evaluator examined the section titled **Idle Session Timeout** in the AGD to verify that it includes instructions for configuring the inactivity time period for remote administrative session termination. Upon investigation, the evaluator found that the AGD states that describes how to set the inactivity period and that the inactivity period is applicable to both remote and local sessions. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3 FTA_SSL.4

5.9.3.1 FTA_SSL.4 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated.
Evaluator Findings	The evaluator examined the **FTA_SSL.4** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies details how the local and remote administrative sessions are terminated. Upon investigation, the evaluator found that the TSS states that: **The TSF allows the administrator to terminate the administrator's own local and remote interactive sessions.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3.2 FTA_SSL.4 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session.
Evaluator Findings	The evaluator examined the section titled **Logging Out** in the AGD to verify that it states how to terminate a local or remote interactive session. Upon investigation, the evaluator found that the AGD contains instructions for logging out of the web GUI (remote) or CLI (remote, local). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.4 FTA_TAB.1

5.9.4.1 FTA_TAB.1 TSS 1

Objective	The evaluator shall check the TSS to ensure that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS). The evaluator shall check the TSS to ensure that all administrative methods of access available to the Security Administrator are listed and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method

	of access. The advisory notice and the consent warning message might be different for different administrative methods of access and might be configured during initial configuration (e.g., via configuration file).
Evaluator Findings	The evaluator examined the **FTA_TAB.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS details each administrative method of access available to the Security Administrator and states that the TOE is displaying an advisory notice and consent warning message for each administrative method of access. Upon investigation, the evaluator found that the TSS states that: **The TSF displays a configurable message before establishing a local or remote administrative session.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.4.2 FTA_TAB.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message.
Evaluator Findings	The evaluator examined the section titled **Set the GUI Banner** and **Set the CLI Banner** in the AGD to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD describes how to configure the banner message for both CLI and web GUI Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10 TSS and Guidance Activities (Trusted Path/Channels)

5.10.1 FTP_ITC.1

5.10.1.1 FTP_ITC.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.
Evaluator Findings	The evaluator examined the **FTP_ITC.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. Upon investigation, the evaluator found that the TSS states that: **The TSF provides a trusted channel with the Syslog server and LDAP server as described in FCS_TLSC_EXT.1.** The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes all secure communication mechanisms in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional

	Requirements listed in the ST. Upon investigation, the evaluator found that the TSS clearly indicates that the connection is via TLS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.1.2 FTP_ITC.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.
Evaluator Findings	The evaluator examined the section titled **Syslog** and **Setup Admin UI Access via LDAP** in the AGD to verify that it contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. Upon investigation, the evaluator found that the AGD describes contains instructions for establishing the allowed protocols with each authorized IT entity. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2 FTP_TRP.1/Admin

5.10.2.1 FTP_TRP.1/Admin TSS 1

Objective	The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.
Evaluator Findings	The evaluator examined the **FTP_TRP.1/Admin** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS indicates the methods of remote TOE administration and how those communications are protected. Upon investigation, the evaluator found that the TSS states that: **The TSF provides a trusted path with remote administrators using TLS/HTTPS as described in FCS_TLSS_EXT.1, FCS_TLSS_EXT.2, and FCS_HTTPS_EXT.1.** The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS protocols are consistent with those specified in the requirement. Upon investigation, the evaluator found that the TSS states that **the TSF provides remote administration using TLS/HTTPS.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2.2 FTP_TRP.1/Admin Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.
Evaluator Findings	The evaluator examined the section titled **Secure Remote Logging, Disable SSH Access, Setup Admin UI Access via LDAP** in the AGD to verify that it contains instructions for establishing the remote administrative sessions for each supported method. Upon investigation, the

	evaluator found that the AGD describes contains instructions for establishing the remote administrative sessions for each supported method. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

NDcPP Test Cases

6.1 FAU_GEN.1 Test #1

<table>
<tr><th>Item</th><th>Data/Description</th></tr>
<tr><td><b>Test ID</b></td><td>FAU_GEN.1 Test#1</td></tr>
<tr><td><b>Objective</b></td><td>The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries.
Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.</td></tr>
<tr><td><b>Test Steps & Expected Test Results</b></td><td>

- **The audit records required for this test case can be found in the test cases associated with each of the**

<table>
<tr><th>Requirement</th><th>Auditable Events</th><th>Additional Audit Record Contents</th><th>Test Steps / Test Case ID</th></tr>
<tr><td>FAU_GEN.1</td><td>• Start-up and shut-down of the audit functions.
• 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</td><td>None.</td><td><b>1. Start-up and shut-down of the audit functions.</b>
<b>Start-up of the audit functions:</b>
<i>Test Steps:</i>
To configure the Syslog server follow the following steps:
2. Go to <b>System Configuration > System Log Files > Syslog Options</b>
3. Add the syslog server IP and select the level of logging.
4. Also add the port number and click on <b>Set Port.</b>
5. Then select the protocol to be used.
Expected output:
When connected to the Syslog server, a successful connection log is generated and the system logs are transferred to the Syslog server.
<b>Shut-down of the audit functions:</b>
<i>Test Steps:</i>
To terminate the Syslog server follow the following steps:</td></tr>
</table>

</td></tr>
</table>

	(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).		1. Go to **System Configuration > System Log Files > Syslog Options** 2. Select **Syslog level** as **None** for the Syslog server that must be removed. Expected output: When terminated the Syslog server, a shutting down connection log is generated and the system logs stop getting transferred to the Syslog server. **3. Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).** **Administrative login:** Test case ID: FTA_SSL.4 Test#2 **Administrative logout:** Test case ID: FTA_SSL.4 Test#2 **4. 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).** **Configuration of new time server:** Test case ID: FCS_NTP_EXT.1.1 Test #1 **Addition of the certificate to the TOE's Trust store:** Test Case ID: FIA_X509_EXT.1.1/Rev Test #1a **Deleting of the certificate from the TOE's Trust store:** Test Case ID: FIA_X509_EXT.1.1/Rev Test #1b **5. 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). Test Case ID: FMT_MTD.1/CryptoKeys Test #2 **6. Resetting passwords (name of related user account shall be logged).** *Test Steps:* To reset the password for a particular user follow the following steps: 1. Go to **System Configuration > System Administration > User Management** 2. From the List of **Local Users** select the user whose password must be reset. 3. Click on **Modify.** 4. Under **Change Password** enter the **New password, Confirm the new password** and click on **Change Password.** Expected output: After the change of password is successful, a log is generated stating the username whose password is set again.
FAU_STG_EXT.3 /LocSpace	Low storage space for audit events.	None.	**Low storage space for audit events** Test Case ID: FAU_STG_EXT.3 /LocSpace
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure	**Failure to establish connection through GUI:** Test Case ID: FIA_UIA_EXT.1 Test #1
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server	**Configuration of new time server:** Test Case ID: FCS_NTP_EXT.1.1 Test #1 **Removal of Time server:** *Test Steps:* To remove a particular NTP host follow the following steps: 1. Go to **System Configuration > System Administration > Date/Time** 2. Remove the current set NTP host and click on **Set NTP host.** Expected output:

			After removing the NTP host a successful execution of the activity log is generated.
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure	**Failure to establish a TLS Session:** Test Case ID: FCS_TLSC_EXT.1.1 Test #2
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure	**Failure to establish a TLS Session:** Test Case ID: FCS_TLSS_EXT.1.1 Test #2
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	**Unsuccessful login attempts limit is met or exceeded:** Test Case ID: FIA_AFL.1 Test #1
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	**Local connection with incorrect credentials:** Test Case ID: FIA_UIA_EXT.1 Test #1 **Local connection with correct credentials:** Test Case ID: FIA_UIA_EXT.1 Test #1 **Remote connection with incorrect credentials:** Test Case ID: FIA_UIA_EXT.1 Test #1 **Remote connection with correct credentials:** Test Case ID: FIA_UIA_EXT.1 Test #1
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	**All use of identification and authentication mechanism** Test Case ID: FIA_UIA_EXT.1 Test #1
FIA_X509_EXT.1 /Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	**Unsuccessful attempt to Validate Certificate:** Test Case ID: FIA_X509_EXT.1.1/Rev Test #1b **Addition of the certificate to the TOE’s Trust store:** Test Case ID: FIA_X509_EXT.1.1/Rev Test #1a **Deleting of the certificate from the TOE’s Trust store:**

			Test Case ID: FIA_X509_EXT.1.1/Rev Test #1b
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.	**Any attempt to initiate a manual update:** Test Case ID: FPT_TUD_EXT.1 Test #1
FMT_SMF.1	All management activities of TSF data.	None.	• **Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1** **Session establishment through WEBUI:** Test Case ID: FIA_UIA_EXT.1 Test #1 **Session establishment through Console:** Test Case ID: FIA_UIA_EXT.1 Test #1 • **Ability to manage the cryptographic keys:** Test Case ID: FMT_MTD.1/CryptoKeys Test #2 • **Ability to configure the cryptographic functionality** Test Case ID: FPT_TUD_EXT.1 Test #1 • **Ability to administer the TOE locally and remotely** **Session establishment through remotely:** Test Case ID: FIA_UIA_EXT.1 Test #1 **Session establishment through locally:** Test Case ID: FIA_UIA_EXT.1 Test #1 • **Ability to configure the access banner** **Through WEBUI:** Test Case ID: FTA_TAB.1 Test #1

			Through Console: Test Case ID: FTA_TAB.1 Test #1 • **Ability to configure the session inactivity time before session termination or locking** **Through WEBUI:** Test Case ID: FTA_SSL.3 Test #1 **Through Console:** Test Case ID: FTA_SSL_EXT.1.1 Test #1 • **Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates** Test Case ID: FPT_TUD_EXT.1 Test #1 • **Ability to configure the authentication failure parameters for FIA_AFL.1** Test Case ID: FIA_AFL.1 Test #1 • **Ability to re-enable an Administrator account** Test Case ID: FIA_AFL.1 Test #2(a) • **Ability to set the time which is used for timestamps** Test Case ID: FPT_STM_EXT.1 Test #1 • **Ability to configure NTP** Test Case ID: FCS_NTP_EXT.1.1 Test #1 • **Ability to manage the TOE's trust store and designate**

			X509.v3 certificates as trust anchors Test Case ID: FIA_X509_EXT.1.1/Rev Test #1a Test Case ID: FIA_X509_EXT.1.1/Rev Test #1b - **Ability to configure the reference identifier for the peer** Test Case ID: FCS_TLSC_EXT.1.2 Test #2 - **Ability to import X.509v3 certificates to the TOE's trust store** - Test Case ID: FIA_X509_EXT.1.1/Rev Test #1a
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.	- **Initiation of update;** Test Case ID: FPT_TUD_EXT.1 Test #1 - **result of the update attempt (success or failure)** Test Case ID: FPT_TUD_EXT.1 Test #1 Test Case ID: FPT_TUD_EXT.1 Test #2 (a)
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	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).	**Manual Setting of Time:** Test Case ID: FPT_STM_EXT.1 Test #1 **Setting of time using NTP:** Test Case ID: FCS_NTP_EXT.1.1 Test #1
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	None.	**The termination of a local session by the session locking mechanism:** **Through Console:**

			Test Case ID: FTA_SSL_EXT.1.1 Test #1
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	**The termination of a remote session by the session locking mechanism:** **Through WEBUI:** Test Case ID: FTA_SSL.3 Test #1
FTA_SSL.4	The termination of an interactive session.	None.	**The termination of an interactive session:** **Console:** Test Case ID: FTA_SSL.4 Test #1 **WEBUI:** Test Case ID: FTA_SSL.4 Test #2
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.	**Initiation of the trusted channel:** Test Case ID: FTP_ITC.1 Test #4 **Termination of the trusted channel:** Test Case ID: FTP_ITC.1 Test #4 **Failure of the trusted channel:** Test Case ID: FIA_X509_EXT.1.1/Rev Test #3
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.	**Initiation of the trusted path:** Test Case ID: FTP_TRP.1/Admin Test #1 **Termination of the trusted path:** *Test Steps:* To terminate the Syslog server, follow the following steps: 1. Go to **System Configuration > System Log Files > Syslog Options** 2. Select **Syslog level** as **None** for the Syslog server that must be removed. Expected output: When terminated the Syslog server a shutting down connection log is generated and the system logs stop

<table>
<tr><td></td><td><table><tr><td></td><td></td><td></td><td>getting transferred to the Syslog server.

<b>Failure of the trusted path functions:</b>
Test Case ID: FIA_X509_EXT.1.1/Rev Test #3</td></tr></table>
<ul><li><b>Provide sample audit logs generated while testing a relevant security function.</b></li><li><b>Verify that each audit record is generated and contains the required information.</b></li></ul></td></tr>
<tr><td><b>Pass/Fail with Explanation</b></td><td>Pass. TOE generates the audit records for the events listed in the table of audit events and administrative actions listed in the table. This meets the testing requirements.</td></tr>
</table>

6.2 FAU_STG_EXT.1 Test #1

Item	**Data**
Test ID	FAU_STG_EXT.1 Test #1
Objective	Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.
Test Steps & Expected Test Results	• Confirm the name and version of the audit server. • Configure the TOE to communicate with a syslog server via TLS. • Generate the audit event and confirm that each event has been logged on the syslog server. • Verify via packet capture that syslog messages have been sent encrypted.
Pass/Fail with Explanation	Pass. The TOE passes all audit traffic to the remote audit server through a secure channel. This meets the testing requirements.

6.3 FAU_STG_EXT.1 Test #2b

Item	**Data**
Test ID	FAU_STG_EXT.1 Test#2b
Objective	Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behavior defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator must check the content of the audit data when the audit data is just filled to the maximum and then verifies that:

	The audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after the local storage for audit data is cleared (for the option '**drop new audit data**' in FAU_STG_EXT.1.3).
Test Steps & Expected Test Results	- Login to the TOE using the xroot access. - Check the disk Usage using df- h. - Now fill up the log partition to about 100% capacity and wait for more than a minute to view the log on the device. - Verify all the log files on TOE stop storing the logs - Verify that even though the local audit are dropped due to storage full, the new audit logs are still generating and transmitted to the external audit server. - Free up space from /var/log partition. - Verify that logging resumed
Pass/Fail with Explanation	Pass. Evaluator verified after the filling the log partition to 100% on the TOE, logs stop getting recorded on the TOE. After freeing some local space, logs starts getting recorded on the TOE. Evaluator also verified that while the local storage is full, the TOE still transmits the newly generated logs to the configured external audit server. This meets the test requirements.

6.4 FAU_STG_EXT.3/LocSpace

Item	**Data**
Test ID	FAU_STG_EXT.3/LocSpace
Objective	The evaluator shall verify that a warning is issued by the TOE before the local storage space for audit data is full.
Test Steps & Expected Test Results	- Login to the TOE using the xroot access. - Check the disk Usage using df- h. - Fill the /var/log/partition upto 84% using the "dd" command: dd bs=1024 count=$((1024 * 1024 * 5)) if=/dev/zero of=bigfile Note: the value (1024 * 1024 * 5) is equivalent to 5GB. The first 1024 is a KB value equivalent to 1 MB. Second 1024 and 5 are just the multiplication factors to provide expected file size. - To update the cron job for log disk usage notification to be executed per minute, edit the file /etc/crontab and find the following line: 0 * * * * root /sbin/check_dskusage >/dev/null 2>&1 Change the "0" to "*", so that it reads as follows: * * * * root /sbin/check_dskusage >/dev/null 2>&1 As a result of this change, no log will appear until disk usage is above 85%. - Now fill up the log partition to about 93% capacity and wait for more than a minute to view the log on the device.
Pass/Fail with Explanation	Pass. Warning is issued by the TOE before the local storage space for audit data is full. This meets the testing requirements.

6.5 FCS_NTP_EXT.1.1 Test #1

Item	**Data**
Test ID	FCS_NTP_EXT.1.1 Test#1
Objective	The version of NTP selected in element 1.1 and specified in the ST shall be verified by observing establishment of a connection to an external NTP server known to be using the specified version(s) of NTP. This may be combined with tests of other aspects of FCS_NTP_EXT.1 as described below.

Test Steps & Expected Test Results	• Configure NTP server on the TOE. • Verify NTP syncs on TOE. • Verify NTP version with packet capture. • Verify the successful logs on the TOE.
Pass/Fail with Explanation	Pass. The TOE uses the correct NTP version specified in the ST. This meets the testing requirement.

6.6 FCS_NTP_EXT.1.2 Test #1

Item	**Data**
Test ID	FCS_NTP_EXT.1.2 Test#1
Objective	[Conditional] If the **message digest algorithm** is claimed in element 1.2, the evaluator will change the message digest algorithm used by the NTP server in such a way that the new value does not match the configuration on the TOE and confirms that the TOE does not synchronize to this time source. The evaluator shall use a packet sniffer to capture the network traffic between the TOE and the NTP server. The evaluator uses the captured network traffic, to verify the NTP version, to observe time change of the TOE and uses the TOE's audit log to determine that the TOE accepted the NTP server's timestamp update. The captured traffic is also used to verify that the appropriate message digest algorithm was used to authenticate the time source and/or the appropriate protocol was used to ensure integrity of the timestamp that was transmitted in the NTP packets. **[TD0639 Applied]**
Test Steps & Expected Test Results	• Configure the TOE for SHA-1. • Configure the NTP server with unsupported message digest by TOE. • Connect the TOE to an NTP server and verify that the synchronization fails. • Verify the connection is refused via packet capture. • Configure the NTP server with supported message digest by TOE. • Connect the TOE to an NTP server and verify that the synchronization succeeds. • Verify the connection is established via packet capture. • Verify the connection is established via logs.
Pass/Fail with Explanation	Pass. The TOE is in sync with NTP Server when supported Message Digest is configured on NTP Server, this satisfies the requirement.

6.7 FCS_NTP_EXT.1.3 Test #1

Item	**Data**
Test ID	FCS_NTP_EXT,1.3 Test#1
Objective	The evaluator shall configure NTP server(s) to support periodic time updates to broadcast and multicast addresses. The evaluator shall confirm the TOE is configured to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. The evaluator shall check that the time stamp is not updated after receipt of the broadcast and multicast packets.
Test Steps & Expected Test Results	Broadcast: • Configure an NTP server to update from a broadcast address. • Configure TOE to future date. • Verify that the TOE does not accept broadcast updates from the NTP server. • Verify with packet capture.

	Multicast: - Configure an NTP server to update from a multicast address. - Check current time on the TOE. - Verify with packet capture that the TOE does not accept multicast updates from the NTP server. - Check new time. There have been no significant changes other than normal passage of time.
Pass/Fail with Explanation	Pass. The TOE does not sync with an NTP server that sends out broadcast updates. This meets testing requirements.

6.8 FCS_NTP_EXT.1.4 Test #1

Item	**Data**
Test ID	FCS_NTP_EXT.1.4 Test#1
Objective	Test 1: The evaluator shall confirm the TOE supports configuration of at least three (3) NTP time sources. The evaluator shall configure at least three NTP servers to support periodic time updates to the TOE. The evaluator shall confirm the TOE is configured to accept NTP packets that would result in the timestamp being updated from each of the NTP servers. The evaluator shall check that the time stamp is updated after receipt of the NTP packets. The purpose of this test to verify that the TOE can be configured to synchronize with multiple NTP servers. It is up to the evaluator to determine that the multi- source update of the time information is appropriate and consistent with the behavior prescribed by the RFC 1305 for NTPv3 and RFC 5905 for NTPv4. **[TD0528 Applied]**
Test Steps & Expected Test Results	- Configure at least 3 NTP time sources on TOE. - Configure the NTP server to use the same key ID. - Start the NTP synchronization and verify that it syncs to NTP server with IP 10.1.3.78 - Verify via packet capture that the TOE has synced to NTP server with IP 10.1.3.78 - Verify via logs that the TOE has synced to NTP server with IP 10.1.3.78 - Stop the previous NTP server and sync with another NTP server with IP 10.1.3.80 - Configure this NTP server to use the same key ID. - Start the NTP synchronization and verify that it syncs to NTP server with IP 10.1.3.80 - Verify via packet capture that the TOE has synced to NTP server with IP 10.1.3.80 - Verify via logs that the TOE has synced to NTP server with IP 10.1.3.80 - Stop the previous NTP server to sync with another NTP server with IP 10.1.1.66 - Configure this NTP server to use the same key ID. - Start the NTP synchronization and verify that it syncs to NTP server with IP 10.1.1.66 - Verify via packet capture that the TOE has synced with NTP server 10.1.1.66 - Verify via logs that the TOE has synced with NTP server 10.1.1.66 - Verify that that the multi- source update of the time information is appropriate and consistent with the behavior prescribed by the RFC 5905
Pass/Fail with Explanation	The TOE successfully handles the use of multiple NTP servers. This meets testing requirements.
Results	Pass

6.9 FCS_NTP_EXT.1.4 Test #2

Item	Data
Test ID	FCS_NTP_EXT.1.4 Test#2
Objective	Test 2: (The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers). The evaluator shall confirm that the TOE would not synchronize to other, not explicitly configured time sources by sending an otherwise valid but unsolicited NTP Server responses indicating different time from the TOE's current system time. This rogue time source needs to be configured in a way (e.g., degrade or disable valid and configured NTP servers) that could plausibly result in unsolicited updates becoming a preferred time source if they are not discarded by the TOE. The TOE is not mandated to respond in a detectable way or audit the occurrence of such unsolicited updates. The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers. It is up to the evaluator to craft and transmit unsolicited updates in a way that would be consistent with the behavior of a correctly functioning NTP server. **[TD0528 Applied]**
Test Steps & Expected Test Results	• Verify the time on the TOE. • Configure an NTP server. • Sync the TOE with NTP server and capture those packets. • Verify with packet capture. • Configure a different NTP server to which the TOE syncs. • Replay the packets from the NTP server which were captured during earlier sync. • Verify the TOE does not sync with the NTP server.
Pass/Fail with Explanation	Pass. The TOE only accepts NTP updates from configured NTP Servers. This meets the testing requirements.

6.10 FPT_STM_EXT.1 Test #1

Item	Data
Test ID	FTP_STM_EXT.1 Test#1
Objective	Test 1: If the TOE supports direct **setting of the time by the Security Administrator** then the evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.
Test Steps & Expected Test Results	• Login into the TOE with correct credentials via GUI. • Confirm the current time on the TOE. • Set a new time on the TOE via the remote GUI. • Verify that the new time is set. • Verify logs were generated for time change.
Pass/Fail with Explanation	Pass. The TOE allows the administrative user to configure the time on the TOE. This meets the testing requirements.

6.11 FPT_STM_EXT.1 Test #2

Item	Data
Test ID	FPT_STM_EXT.1 Test#2
Objective	Test 2: If the TOE supports the **use of an NTP server**; the evaluator shall use the guidance documentation to configure the NTP client on the TOE and set up a communication path with

	the NTP server. The evaluator will observe that the NTP server has set the time to what is expected. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the guidance documentation.
Test Steps & Expected Test Results	• Confirm the current time on the TOE. • Configure NTP support on the TOE via the remote console over GUI. • Verify that the new time is set. • Verify that the TOE time matches with the NTP server. • Verify via logs that the TOE synchronizes with the NTP server.
Pass/Fail with Explanation	Pass. The TOE was successfully able to synchronize with the NTP server. This meets the testing requirements.

6.12 FTP_ITC.1 Test #1

Item	Data
Test ID	FTP_ITC_.1 Test#1
Objective	The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps	FAU_STG_EXT.1 and FCS_TLSC_EXT.1 covers this test requirements.
Pass/Fail with Explanation	Pass. The TOE can be configured to successfully communicate with the external authentication server via LDAP Authentication and syslog server over TLS. This meets the testing requirements.

6.13 FTP_ITC.1 Test #2

Item	Data
Test ID	FTP_ITC_.1 Test#2
Objective	For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.
Test Steps	FAU_STG_EXT.1 and FCS_TLSC_EXT.1 covers this test requirements.
Pass/Fail with Explanation	Pass. The TOE can be configured to successfully communicate with the external authentication server via LDAP Authentication and syslog server over TLS. This meets the testing requirements.

6.14 FTP_ITC.1 Test #3

Item	Data
Test ID	FTP_ITC_.1 Test#3
Objective	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Test Steps	FAU_STG_EXT.1 and FCS_TLSC_EXT.1 covers this test requirements.
Pass/Fail with Explanation	Pass. External connections from the TOE are sent via an encrypted channel. This meets the testing requirements.

6.15 FTP_ITC.1 Test #4

Item	Data
Test ID	FTP_ITC_.1 Test#3

Objective	Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities. The evaluator shall, for each instance where the TOE acts as a client utilizing a secure communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations: 1. A duration that exceeds the TOE's application layer timeout setting, 2. A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer. The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext. In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g., a core switch) shall be used to interrupt the connection between the TOE and the distinct IT entity. The interruption shall not be performed at the virtual node (e.g., virtual switch) and must be physical in nature.
Test Steps & Expected Test Results	• Configure and ensure a successful TLS connection with an IT entity. • Set the timeout value to 120 seconds. • Interrupt the connection between the devices for a duration shorter than the application layer timeout but of sufficient length to interrupt the Network link layer (less than 120 seconds) and verify that connection is down. • Verify that the traffic is encrypted when connection was restored. • Verify the connection time with TOE Logs. • Interrupt the connection between the devices for a duration that exceeds the TOE's application layer timeout setting (more than 120 seconds) and verify that connection is down. • Verify that the traffic is encrypted when connection was restored. • Verify the connection time with TOE Logs.
Pass/Fail with Explanation	Pass. The TOE does not send plaintext traffic when disconnected from the log server. This meets the testing requirements.

6.16 FCS_HTTPS_EXT.1 Test#1

Item	**Data**
Test ID	FCS_HTTPS_EXT.1 Test#1
Objective	This test is now performed as part of FIA_X509_EXT.1/Rev testing. Tests are performed in conjunction with the TLS evaluation activities. If the TOE is an HTTPS client or an HTTPS server utilizing X.509 client authentication, then the certificate validity shall be tested in accordance with testing performed for FIA_X509_EXT.1.
Pass/Fail with Explanation	NA.TOE is a HTTPS server without mutual authentication.

6.17 FIA_AFL.1 Test #1

Item	**Data**
Test ID	FIA_AFL_.1 Test#1
Objective	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g., any passwords entered as part of establishing the connection protocol or the remote administrator application):

	Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE (and, if the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall also use the operational guidance to configure the time period after which access is re-enabled). The evaluator shall test that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful.
Test Steps & Expected Test Results	• Configure the number of failure attempts to 3 before being locked out. • Confirm the configuration has been implemented in the config. • Authenticate and verify correct credentials result in a successful connection. • Verify the connection is established via logs. • Attempt to connect to the TOE with incorrect credentials. • Verify that attempts with unsuccessful credentials will be rejected. • Attempt to connect to the TOE with correct credentials. • Verify that attempts with successful credentials will be rejected after the authentication failure limit is reached.
Pass/Fail with Explanation	Pass. The TOE adheres to the threshold and lockout policies defined by the administrator.

6.18 FIA_AFL.1 Test #2a

Item	Data
Test ID	FIA_AFL_.1 Test#2a
Objective	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g., any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows: If the **administrator action** selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall confirm by testing that following the operational guidance and performing each action specified in the ST to re-enable the remote administrator's access results in successful access (when using valid credentials for that administrator).
Test Steps & Expected Test Results	HTTPS: • Login into the TOE using the administrator account. • Verify after the final attempt that the user account is now locked out. • Verify that the user account is locked out via Log. • Manually unlock the user account using the administrator account. • Verify the user was unblocked via logs. • Authenticate and verify correct credentials result in a successful connection. • Verify the connection is established via logs.
Pass/Fail with Explanation	Pass. Authentication failure disallows user from validating after configured number of failed attempts and manually re-enable the remote administrator's access (via WEBUI) results in successful access.

6.19 FIA_PMG_EXT.1 Test #1

Item	Data
Test ID	FIA_PMG_EXT.1 Test #1
Objective	The evaluator shall compose passwords that meet the requirements in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator

	is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, and a minimum length listed in the requirement are supported and justify the subset of those characters chosen for testing.
Test Steps & Expected Test Results	• Set the minimum password length to 8 characters. • Verify via logs that the configuration is updated. • Create a user “good1” with a combination of lowercase, uppercase letters, numbers and special characters --- {QweRty!@#$%^789} • Verify that the new user has been created. • Verify via logs that the user has been created. • Log into the TOE using the good1 user. • Verify that the user was able to get the access to the TOE. • Verify via logs that the user successfully logged in to the TOE. • Create a user “good2” with a combination of lowercase, uppercase letters, numbers and special characters--- “(‘Sun,456-./’)&*+;” • Verify that the new user has been created. • Verify via logs that the user has been created. • Log into the TOE using the good2 user. • Verify that the user was able to get the access to the TOE. • Verify via logs that the user successfully logged in to the TOE. • Create a user “good3” with a combination of lowercase, uppercase letters, numbers and special characters--- [“m0on”:<+?>123_`~|] • Verify that the new user has been created. • Verify via logs that the user has been created. • Log into the TOE using the good3 user. • Verify that the user was able to get the access to the TOE. • Verify via logs that the user successfully logged in to the TOE. • Create a user “good4” only with lowercase characters “aaaaaaaa”. • Verify that the new user is not created. • Create a user “good5” only with lowercase characters “abcdefgh”. • Verify that the new user is not created.
Pass/Fail with Explanation	Pass. The TOE was able to create users with good passwords. This meets the testing requirements.

6.20 FIA_PMG_EXT.1 Test #2

Item	**Data**
Test ID	FIA_PMG_EXT.1 Test #2
Objective	The evaluator shall compose passwords that do not meet the requirements in some way. For each password, the evaluator shall verify that the TOE does not support the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that the TOE enforces the allowed characters and the minimum length listed in the requirement and justify the subset of those characters chosen for testing.
Test Steps & Expected Test Results	• Set the minimum password length to 8 characters. • Verify via logs that the configuration is updated. • Create a user “bad1” with 7 characters using the combination of lowercase and uppercase letters and numbers “12390Rt”. • Verify that the user is not created.

	• Create a user “bad2” with 6 characters using numbers and special characters “12%$34”. • Verify that the user is not created. • Create a user “bad3” with 4 characters using the combination of lowercase, uppercase letters, numbers and special characters “A#1k”. • Verify that the new user is not created.
Pass/Fail with Explanation	Pass. The TOE was able to reject users with bad passwords. This meets the testing requirements.

6.21 FIA_UIA_EXT.1 Test #1

Item	**Data**
Test ID	FIA_UIA_EXT.1 Test #1
Objective	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 1: The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.
Test Steps & Expected Test Results	Console: • Attempt to login from a local connection with incorrect credentials. • Confirm that access was denied. • Verify that an audit record was generated showing login failure. • Log into the TOE from a local connection with correct credentials. • Confirm that access was granted. • Verify that an audit record was generated showing login success. GUI: • Attempt to login from a remote GUI connection with incorrect credentials. • Confirm that access was denied. • Verify that an audit record was generated showing login failure. • Log into the TOE from a remote GUI connection with correct credentials. • Confirm that access was granted. • Verify that an audit record was generated showing login success.
Pass/Fail with Explanation	Pass. Presenting incorrect authentication credentials results in denied access to the TOE. Presenting correct authentication credentials results in access being allowed to the TOE. This meets the testing requirements.

6.22 FIA_UIA_EXT.1 Test #2

Item	**Data**
Test ID	FIA_UIA_EXT.1 Test #2
Objective	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 2: The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.

Test Steps & Expected Test Results	**1. Display the warning banner in accordance with FTA_TAB.1:** - Show that commands are not available prior to login and verify that the login banner is displayed. - Verify that after clicking 'Accept' icon, the page will be displayed asking for login credentials and no other system services can be accessed. - Login into the TOE via GUI. - Verify that the services are available after the login. - Verify authentication logs reflect success. **2. Automated generation of cryptographic keys:** - This requirement is fulfilled in accordance with test FPT_TUD_EXT.1 Test#1. In the logs, we can see that the TOE generated a self-signed certificate key after a successful reboot after updating the software. **Remote CLI:** **1. Display the warning banner in accordance with FTA_TAB.1:** - Verify that no functionality except those specified in the requirement is allowed. - Verify that when connected via CLI, the TOE displays the login banner and asks for login credentials and no other system services can be accessed. - Login into the TOE via CLI. - Verify that the services are available after the login. - Verify authentication logs reflect success.
Pass/Fail with Explanation	Pass. No system services are available to an unauthenticated user connecting remotely. This meets the testing requirements.

6.23 FIA_UIA_EXT.1 Test #3

Item	Data
Test ID	FIA_UIA_EXT.1 Test #3
Objective	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.
Test Steps & Expected Test Results	- Connect to the TOE via local console and verify the only option presented is the username/password entry.
Pass/Fail with Explanation	Pass. The login banner is displayed. Other system services can be accessed prior to login.

6.24 FIA_UAU.7 Test #1

Item	Data
Test ID	FIA_UAU.7 Test #1
Objective	The evaluator shall perform the following test for each method of local login allowed: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.

Test Steps & Expected Test Results	- Attempt to login via local console. Note that the password is invisible. - Verify the successful connection via logs. - Attempt to login via web GUI. Note that the password is invisible. - Verify the successful connection via logs.
Pass/Fail with Explanation	Pass. At both the directly connected and remote login prompt, the TOE does not provide anything more than obscured feedback. This meets the testing requirements.

6.25 FMT_MOF.1/ManualUpdate Test #1

Item	**Data**
Test ID	FMT_MOF.1/ManualUpdate Test#1
Objective	The evaluator shall try to perform the update using a legitimate update image without prior authentication as Security Administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail.
Test Steps & Expected Test Results	- Create an unprivileged user on the TOE. - Verify the user was created. - Verify the user was created via logs. - Login into the TOE with unprivileged user. - Verify that the user does not have the privilege to perform manual update on the TOE. - Login with privileged user on the TOE and show the option to perform manual update is available.
Pass/Fail with Explanation	Pass. An unprivileged user cannot perform a software update on the TOE. This meets the testing requirements.

6.26 FMT_MOF.1/ManualUpdate Test #2

Item	**Data**
Test ID	FMT_MOF.1/ManualUpdate Test#2
Objective	The evaluator shall try to perform the update with prior authentication as Security Administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already.
Test Steps	Authenticated user can configure trusted update. This test case is covered by the test for FPT_TUD_EXT.1 Test #1. This meets the testing requirements
Pass/Fail with Explanation	Pass. Authenticated user can configure trusted update. This test case is covered by the test for FPT_TUD_EXT.1 Test #1. This meets the testing requirements

6.27 FMT_MTD.1/CryptoKeys Test #1

Item	**Data**
Test ID	FMT_MTD.1/CrytoKeys Test#1
Objective	The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access

	control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps & Expected Test Results	Crypto Key Generation using CSR: • Login into the TOE with unprivileged user. • Attempt to generate the crypto keys by generating a CSR request; this should fail. • Verify the generation of CSR fails for unprivileged user. Crypto Key Generation using Self-signed certificate: • Login into the TOE with unprivileged user. • Verify that the user does not have the privilege to generate crypto keys using self-signed certificate generation; this should fail**.**
Pass/Fail with Explanation	Failed. Unprivileged user cannot generate the crypto keys using the Certificate Signing Requests and self-signed certificates.

6.28 FMT_MTD.1/CryptoKeys Test #2

Item	**Data**
Test ID	FMT_MTD.1/CrytoKeys Test#2
Objective	The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.
Test Steps & Expected Test Results	Crypto Key Generation using CSR: • Login into the TOE with a privileged user. • Verify the generation of CSR passes for privileged user. • Verify via logs that the privileged user can generate CSR. Crypto Key Generation using Self-signed certificate: • Login into the TOE with privileged user. • Attempt to generate crypto keys using self-signed certificate generation; this will pass. • Verify the generation is successful via logs.
Pass/Fail with Explanation	Pass. Authorized user can perform security related configurations on the TOE. This meets the testing requirements.

6.29 FMT_SMF.1 Test #1

Item	**Data**
Test ID	FMT_SMF.1 Test#1
Objective	The evaluator tests management functions as part of testing the SFRs identified in section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR.
Note	**FMT_SMF.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;* • [○ *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*

	○ *Ability to manage the cryptographic keys;* ○ *Ability to configure the cryptographic functionality;* ○ *Ability to re-enable an Administrator account;* ○ *Ability to set the time which is used for time-stamps;* ○ *Ability to configure NTP;* ○ *Ability to configure the reference identifier for the peer;* ○ *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;* ○ *Ability to import X.509v3 certificates to the TOE's trust store;* ○]
Test Steps	N/A – All management functions were tested as part of testing in other SFRs
Pass/Fail with Explanation	Pass. Throughout the various security functionality testing of the TOE, FMT_SMF.1 Specification of Management Functions requirements have been met. Therefore, this test Passed.

6.30 FMT_SMR.2 Test #1

Item	**Data**
Test ID	FMT_SMR.2 Test#1
Objective	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.
Test Steps	As there are two interfaces where these can be tested (over the GUI/Console) and all test cases are tested that way. The evaluator has met this requirement through execution of the entirety of this test report for the TOE interfaces.
Pass/Fail with Explanation	Pass. As there are two interfaces where these can be tested (over the GUI/Console) and all test cases are tested that way. The evaluator has met this requirement through execution of the entirety of this test report for the TOE interfaces.

6.31 FTA_SSL.3 Test #1

Item	**Data**
Test ID	FTA_SSL.3 Test#1
Objective	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Test Steps & Expected Test Results	• Configure a remote GUI time out period of 1 minute on administrative sessions. • Login onto the TOE via GUI. • Let the remote GUI connection set idle for 1 minute. • Verify that the session was terminated. • Verify that a log was created for the configuring the timeout period. • Verify that a log was created for inactivity logout. • Configure a remote GUI time out period of 2 minute on administrative sessions. • Login onto the TOE via GUI.

	- Let the remote GUI connection set idle for 2 minutes. - Verify that the session was terminated. - Verify that a log was created for the configuring the timeout period. - Verify that a log was created for inactivity logout.
Pass/Fail with Explanation	Pass. The remote administrative time out periods can be set by the administrative user. The TOE enforces the configured inactivity period in each instance. This meets the testing requirements.

6.32 FTA_SSL.4 Test #1

Item	**Data**
Test ID	FTA_SSL.4 Test#1
Objective	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps & Expected Test Results	- Log into the TOE through a local administrative interface. - Verify the logs reflect log in. - Using the instructions provided by the user guide log off. - Verify the logs reflect the log off.
Pass/Fail with Explanation	Pass. The TOE allows user to terminate the directly connected administrative sessions. This meets the testing requirements.

6.33 FTA_SSL.4 Test #2

Item	**Data**
Test ID	FTA_SSL.4 Test#2
Objective	The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps & Expected Test Results	- Login onto the TOE through the remote GUI. - Verify via logs that the user has logged in. - Using the instructions provided by the user guide log off. - Verify via logs that the user has logged out.
Pass/Fail with Explanation	Pass. The TOE allows user to terminate the remote administrative sessions. This meets the testing requirements.

6.34 FTA_SSL_EXT.1.1 Test #1

Item	**Data**
Test ID	FTA_SSL.EXT.1.1 Test#1
Objective	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.

Test Steps & Expected Test Results	• Configure a local time out period of 1 min on administrative sessions from the local console. • Log into the TOE via local console. • Let the console connection set idle for 1 minute. • Verify that the session was terminated. • Verify that a log was created for the configuring the timeout period. • Verify that a log was created for inactivity logout. • Configure a local time out period of 2 mins on administrative sessions from the local console. • Log into the TOE via local console. • Let the console connection set idle for 2 minutes. • Verify that the session was terminated. • Verify that a log was created for the configuring the timeout period. • Verify that a log was created for inactivity logout.
Pass/Fail with Explanation	Pass. The local administrative inactivity was able to be set to multiple values. In each instance, the TOE logged the user out after the configured time.

6.35 FTA_TAB.1 Test #1

Item	Data
Test ID	FTA_TAB.1 Test#1
Objective	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.
Test Steps & Expected Test Results	GUI: • Configure access banners on TOE via GUI. • Verify that the banner is being displayed in GUI while login. • Verify the logs generated for the configuration steps. Console: • Configure access banners on TOE via GUI. • Verify that the banner is being displayed while login. • Verify the logs generated for the configuration steps.
Pass/Fail with Explanation	Pass. For both GUI and Console the banner is getting displayed.

6.36 FTP_TRP.1/Admin Test #1

Item	Data
Test ID	FTP_TRP.1/Admin Test #1
Objective	The evaluators shall ensure that communications using each specified (in the guidance documentation) remote administration method is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps & Expected Test Results	• Log into the TOE via GUI. • Verify audit logs that user is successfully logged in to the TOE. • Verify that the session was established, and data is encrypted via packet capture.

Pass/Fail with Explanation	Pass. Remote administrative access to the TOE is over secured channels. This meets the testing requirements.

6.37 FTP_TRP.1/Admin Test #2

Item	**Data**
Test ID	FTP_TRP.1/Admin Test #2
Objective	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
Test Steps	This test is performed in conjunction with FTP_TRP.1/Admin Test #1 test. Remote administrative access to the TOE is over secured channels and the data was not sent in plaintext. This meets the testing requirements.
Pass/Fail with Explanation	Pass. This test is performed in conjunction with FTP_TRP.1/Admin Test #1 test. Remote administrative access to the TOE is over secured channels and the data was not sent in plaintext. This meets the testing requirements.

6.38 FCS_TLSC_EXT.1.1 Test #1

Item	**Data**
Test ID	FCS_TLSC_EXT.1.1 Test #1
Objective	The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Steps & Expected Test Results	• Configure the TOE to connect to the TLS server. • Attempt the connection from the TOE to the TLS Server using the cipher TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA. • Verify the with packet capture the required ciphersuite is TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA. • Attempt the connection from the TOE to the TLS Server using the cipher TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA. • Verify the with packet capture the required ciphersuite is TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA. • Attempt the connection from the TOE to the TLS Server using the cipher TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. • Verify the with packet capture the required ciphersuite is TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. • Attempt the connection from the TOE to the TLS Server using the cipher TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384. • Verify the with packet capture the required ciphersuite is cipher TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384. • Attempt the connection from the TOE to the TLS Server using the cipher TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256. • Verify the packet capture the required ciphersuite is cipher TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256. • Attempt the connection from the TOE to the TLS Server using the cipher TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

	• Verify the packet capture the required ciphersuite is cipher TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.
Pass/Fail with Explanation	Pass. TOE successfully negotiates each of the claimed cipher suites. This meets the test requirements.

6.39 FCS_TLSC_EXT.1.1 Test #2

Item	Data
Test ID	FCS_TLSC_EXT.1.1 Test #2
Objective	The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field, and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
Test Steps & Expected Test Results	Valid Certificate: • Load the server certificate containing the Server Authentication purpose on the TLS server. • Attempt the connection from the TOE to the TLS Server. • Verify the successful connection with packet capture. Invalid Certificate: • Load the server certificate lacking the Server Authentication purpose on the TLS server. • Attempt the connection from the TOE to the TLS Server. • Verify the error with logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE does not make the connection because the evaluation of the extended keyusage field fails. This meets the test requirements.

6.40 FCS_TLSC_EXT.1.1 Test #3

Item	Data
Test ID	FCS_TLSC_EXT.1.1 Test #3
Objective	The evaluator shall send a server certificate in the TLS connection that the does not match the server-selected ciphersuite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite). The evaluator shall verify that the TOE disconnects after receiving the server’s Certificate handshake message.
Test Steps & Expected Test Results	• Start the connection using the ‘Acumen-TLSC’ tool with an RSA certificate and ECDSA cipher suite. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE denied a connection to a server using a certificate that doesn’t match the cipher suite. This meets the test requirements.

6.41 FCS_TLSC_EXT.1.1 Test #4a

Item	Data
Test ID	FCS_TLSC_EXT.1.1 Test #4a

Objective	The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.
Test Steps & Expected Test Results	• Start the connection using the 'Acumen-TLS' tool with TLS_NULL_WITH_NULL NULL cipher suite. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE does not complete the session because TLS_NULL_WITH_NULL_NULL is presented. This meets the test requirements.

6.42 FCS_TLSC_EXT.1.1 Test #4b

Item	**Data**
Test ID	FCS_TLSC_EXT.1.1 Test #4b
Objective	Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.
Test Steps & Expected Test Results	• Use the 'Acumen-tlsc' tool to initiate a connection and verify the connection with an unsupported ciphersuite. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The console output shows the Acumen-TLS tool modifying the servers selected cipher suite in the Server Hello message to one that is not present in the Client Hello. The TOE rejects the connection by sending a Fatal Alert. This meets the test requirements.

6.43 FCS_TLSC_EXT.1.1 Test #4c

Item	**Data**
Test ID	FCS_TLSC_EXT.1.1 Test #4c
Objective	[conditional]: If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension** the evaluator shall configure the server to perform an ECDHE or DHE key exchange in the TLS connection using a non-supported curve/group (for example P-192) and shall verify that the TOE disconnects after receiving the server's Key Exchange handshake message
Test Steps & Expected Test Results	• Use 'Acumen-tlsc' tool to initiate a connection and verify the connection with an unsupported elliptical curve. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. When configured the server to perform an ECDHE key exchange in the TLS connection using a non-supported curve the connection fails. This meets the requirements.

6.44 FCS_TLSC_EXT.1.1 Test #5a

Item	**Data**
Test ID	FCS_TLSC_EXT.1.1 Test #5a
Objective	Change the TLS version selected by the server in the Server Hello to a non-supported TLS version and verify that the client rejects the connection.
Test Steps & Expected Test Results	• Attempt the connection from the TOE to the TLS Server using the unsupported TLSv1.0 and verify the connection. • Verify the error logs on the device.

	• Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The connection fails due to unsupported TLS version. This meets the test requirements.

6.45 FCS_TLSC_EXT.1.1 Test #5b

Item	**Data**
Test ID	FCS_TLSC_EXT.1.1 Test #5b
Objective	[conditional]: If **using DHE or ECDH**, modify the signature block in the Server's Key Exchange handshake message, and verify that the handshake does not finished successfully, and no application data flows. This test does not apply to cipher suites using RSA key exchange. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.
Test Steps & Expected Test Results	• Use 'Acumen-tlsc' tool to initiate a connection and verify the connection when a byte is modified in the Server's Key Exchange handshake message. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The connection fails due to the modified block in the Server Key Exchange message. This meets the test requirement.

6.46 FCS_TLSC_EXT.1.1 Test #6a

Item	**Data**
Test ID	FCS_TLSC_EXT.1.1 Test #6a
Objective	Modify a byte in the Server Finished handshake message and verify that the handshake does not finish successfully, and no application data flows.
Test Steps & Expected Test Results	• Use the 'Acumen-tlsc' tool to initiate a connection and verify the connection when a byte is modified in the server finished handshake. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The connection is not completed when a corrupted Server Finished message is received. This meets the test requirements.

6.47 FCS_TLSC_EXT.1.1 Test #6b

Item	**Data**
Test ID	FCS_TLSC_EXT.1.1 Test #6b
Objective	Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the handshake does not finish successfully, and no application data flows
Test Steps & Expected Test Results	• Use the 'Acumen-tlsc' tool to initiate a connection and verify the connection when a byte is modified in the server's nonce in the Server Hello handshake message. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE closes the connection after receiving garbled data. This meets the test requirements.

6.48 FCS_TLSC_EXT.1.1 Test #6c

Item	Data
Test ID	FCS_TLSC_EXT.1.1 Test #6c
Objective	Modify at least one byte in the server's nonce in the Server Hello handshake message and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message.
Test Steps & Expected Test Results	• Use the 'Acumen-tlsc' tool to initiate a connection and verify the connection when a byte is modified in the server's nonce in the Server Hello handshake message. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The connection was rejected due to a modified nonce. This meets the test requirements.

6.49 FCS_TLSC_EXT.1.2 Test #1

Item	Data
Test ID	FCS_TLSC_EXT.1.2 Test #1
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each identifier type (e.g., IPv4, IPv6, FQDN) supported in the CN. When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the CN. Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 1.
Test Steps & Expected Test Results	CN as IPV4: • Configure the TOE for reference identifier name as IPV4. • Configure the Server certificate showing bad CN. • Configure the Server certificate showing no SAN extension. • Load the certificate with Bad CN and No SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the connection failure logs on the device which states that CN does not match in peer certificate. • Verify the unsuccessful connection due to bad CN in packet capture. CN as FQDN: • Configure the TOE for reference identifier name as FQDN. • Configure the Server certificate showing bad CN. • Configure the Server certificate showing no SAN extension. • Load the certificate with Bad CN and No SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the connection failure logs on the device which states that CN does not match in peer certificate.

	- Verify the unsuccessful connection due to bad CN in packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects certificates with a bad CN and No SAN. This meets the testing requirements.

6.50 FCS_TLSC_EXT.1.2 Test #2

Item	**Data**
Test ID	FCS_TLSC_EXT.1.2 Test #2
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, URI). When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the SAN.
Test Steps & Expected Test Results	CN and SAN as IPV4: • Configure the TOE for reference identifier name as IPV4. • Configure the Server certificate showing good CN. • Configure the Server certificate showing bad SAN. • Load the certificate with Good CN and Bad SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the connection failure logs on the device which states that SAN does not match in peer certificate. • Verify the unsuccessful connection due to bad SAN but the CN matches with reference identifier in packet capture. CN and SAN as FQDN: • Configure the TOE for reference identifier name as FQDN. • Configure the Server certificate showing good CN. • Configure the Server certificate showing bad SAN. • Load the certificate with Good CN and Bad SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the connection failure logs on the device which states that SAN does not match in peer certificate. • Verify the unsuccessful connection due to bad SAN but the CN matches with reference identifier in packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects certificates with a good CN but bad SAN. This meets the testing requirements.

6.51 FCS_TLSC_EXT.1.2 Test #3

Item	**Data**
Test ID	FCS_TLSC_EXT.1.2 Test #3
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain

	the SAN extension. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each identifier type (e.g., IPv4, IPv6, FQDN) supported in the CN. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted.
Test Steps & Expected Test Results	CN as IPV4: - Configure the TOE for reference identifier name as IPV4. - Configure the Server certificate showing good CN. - Configure the Server certificate showing no SAN extension. - Load the certificate with Good CN and no SAN on TLS server. - Initiate the connection from the TOE to the TLS Server and verify the connection. - Verify the successful connection due to CN matches the reference identifier on the TOE but no SAN present in certificate in packet capture. CN as FQDN: - Configure the TOE for reference identifier name as FQDN. - Configure the Server certificate showing good CN. - Configure the Server certificate showing no SAN extension. - Load the certificate with Good CN and no SAN on TLS server. - Initiate the connection from the TOE to the TLS Server and verify the connection. - Verify the successful connection due to CN matches the reference identifier on the TOE but no SAN present in certificate in packet capture.
Pass/Fail with Explanation	Pass. The TOE successfully accepts the connection when the certificate with a good CN and No SAN is presented. This meets the testing requirements.

6.52 FCS_TLSC_EXT.1.2 Test #4

Item	**Data**
Test ID	FCS_TLSC_EXT.1.2 Test #4
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each supported SAN type (e.g., IPv4, IPv6, FQDN, SRV).
Test Steps & Expected Test Results	CN and SAN as IPV4: - Configure the TOE for reference identifier name as IPV4. - Configure the Server certificate showing bad CN. - Configure the Server certificate showing good SAN extension. - Load the certificate with bad CN and good SAN on TLS server. - Initiate the connection from the TOE to the TLS Server and verify the connection. - Verify the successful connection due to SAN matches the reference identifier on the TOE but a bad CN in packet capture. CN and SAN as FQDN: - Configure the TOE for reference identifier name as FQDN. - Configure the Server certificate showing bad CN. - Configure the Server certificate showing good SAN extension. - Load the certificate with bad CN and good SAN on TLS server. - Initiate the connection from the TOE to the TLS Server and verify the connection.

	- Verify the successful connection due to SAN matches the reference identifier on the TOE but a bad CN in packet capture.
Pass/Fail with Explanation	Pass. The TOE successfully accepts the connection when the certificate with a bad CN and good SAN is presented. This meets the testing requirements.

6.53 FCS_TLSC_EXT.1.2 Test #5 (1)

Item	**Data**
Test ID	FCS_TLSC_EXT.1.2 Test #5 (1)
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e., CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g., foo.*.example.com) and verify that the connection fails.
Test Steps & Expected Test Results	CN: - Configure the TOE for the correct reference identifier. - Configure the node certificate showing wildcard that is not in the left-most label of CN. - Load the certificate showing wildcard that is not in the left-most label of CN on the TLS server. - Initiate the connection from the TOE to the TLS Server and verify the connection. - Verify the error logs on the device due to CN mismatch. - Verify the unsuccessful connection with packet capture. SAN: - Configure the TOE for the correct reference identifier. - Configure the node certificate showing wildcard that is not in the left-most label of SAN. - Load the certificate showing wildcard that is not in the left-most label of SAN on the TLS server. - Initiate the connection from the TOE to the TLS Server and verify the connection. - Verify the error logs on the device due to SAN mismatch. - Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. TOE rejects the connection when the reference identifier does not match the presented wildcard which is not in the leftmost label. This meets the testing requirements.

6.54 FCS_TLSC_EXT.1.2 Test #5 (2)(a)

Item	**Data**
Test ID	FCS_TLSC_EXT.1.2 Test #5 (2)(a)
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e., CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g., *.example.com).

	The evaluator shall configure the reference identifier with a single left-most label (e.g., foo.example.com) and verify that the connection succeeds, if wildcards are supported, or fails if wildcards are not supported. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps & Expected Test Results	CN: - Configure the TOE for the reference identifier with single left-most label. - Configure the node certificate showing wildcard in the leftmost label in CN. - Load the certificate with Wildcard in leftmost label in CN on the TLS server. - Initiate the connection from the TOE to the TLS Server and verify the connection. - Verify the successful connection via packet capture. SAN: - Configure the TOE for the reference identifier with single left-most label. - Configure the node certificate showing wildcard in the leftmost label in SAN. - Load the certificate with Wildcard in leftmost label in SAN on the TLS server. - Initiate the connection from the TOE to the TLS Server and verify the connection. - Verify the successful connection via packet capture.
Pass/Fail with Explanation	Pass. TOE accepts the connection when the reference identifier with single left-most labels is presented in the certificate. This meets the testing requirements.

6.55 FCS_TLSC_EXT.1.2 Test #5 (2)(b)

Item	**Data**
Test ID	FCS_TLSC_EXT.1.2 Test #5 (2)(b)
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e., CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g., *.example.com). The evaluator shall configure the reference identifier without a left-most label as in the certificate (e.g., example.com) and verify that the connection fails. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps & Expected Test Results	CN: - Configure the TOE for the reference identifier without a leftmost label. - Configure the node certificate showing wildcard in the leftmost label in CN. - Load the certificate with Wildcard in leftmost label in CN on the TLS server. - Initiate the connection from the TOE to the TLS Server and verify the connection. - Verify the error logs on the device due to CN mismatch. - Verify the unsuccessful connection with packet capture. SAN: - Configure the TOE for the reference identifier without a leftmost label.

	• Configure the node certificate showing wildcard in the leftmost label in SAN. • Load the certificate with Wildcard in leftmost label in SAN on the TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the error logs on the device due to SAN and reference identifier mismatch. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. When configure the reference identifier with no left-most labels on TOE the connections fail. This meets the testing requirements.

6.56 FCS_TLSC_EXT.1.2 Test #5 (2)(c)

Item	**Data**
Test ID	FCS_TLSC_EXT.1.2 Test #5 (2)(b)
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e., CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g., *.example.com). The evaluator shall configure the reference identifier with two left-most labels (e.g., bar.foo.example.com) and verify that the connection fails. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps & Expected Test Results	CN: • Configure the TOE for the reference identifier with two leftmost labels. • Configure the node certificate showing wildcard in the leftmost label in CN. • Load the certificate with leftmost label in CN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the failure logs on the TOE. • Verify the unsuccessful connection via packet capture. SAN: • Configure the TOE for the reference identifier with two leftmost labels. • Configure the node certificate showing wildcard in the leftmost label in SAN. • Load the certificate with leftmost label in SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the failure logs on the TOE. • Verify the unsuccessful connection via packet capture.
Pass/Fail with Explanation	Pass. When configure the reference identifier with two left-most labels on TOE the connections fail. This meets the testing requirements.
Result	

6.57 FCS_TLSC_EXT.1.2 Test #6

Item	**Data**
Test ID	FCS_TLSC_EXT.1.2 Test #6

Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT**. Test 6: [conditional] If IP address identifiers supported in the SAN or CN, the evaluator shall present a server certificate that contains a CN that matches the reference identifier, except one of the groups has been replaced with a wildcard asterisk (*) (e.g. CN=*.168.0.1 when connecting to 192.168.0.20, CN=2001:0DB8:0000:0000:0008:0800:200C:* when connecting to 2001:0DB8:0000:0000:0008:0800:200C:417A). The certificate shall not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported IP address version (e.g., IPv4, IPv6). Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 6. **[TD 0634 applied]**
Test Steps & Expected Test Results	IPv4: • Configure the TOE for the correct reference identifier. • Create a server certificate with a CN that matches the reference identifier but replace one of the groups with an *. • Load the certificate on the TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the failure logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. TOE rejects the connection when configured server certificate that contains a CN that matches the reference identifier IP except one of the groups has been replaced with an asterisk (*). This meets the test requirements.

6.58 FCS_TLSC_EXT.1.3 Test #1

Item	**Data**
Test ID	FCS_TLSC_EXT.1.3 Test #1
Objective	Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.
Test Steps & Expected Test Results	• Configure TOE to connect to the TLS server. • Create a full chain of certificates to connect to the TOE. • Upload a complete certificate validation chain to the TOE. • Attempt the connection from the TOE to the TLS server and verify the connection (complete certificate chain present). • Verify the successful connection with packet capture.
Pass/Fail with Explanation	Pass. When a complete certificate trust chain is present, the TOE can make a successful connection. This meets the test requirements.

6.59 FCS_TLSC_EXT.1.3 Test #2

Item	**Data**
Test ID	FCS_TLSC_EXT.1.3 Test #2

Objective	The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g., trusted channel was established) covering the types of failure for which an override mechanism is defined.
Test Steps & Expected Test Results	Failed matching reference Identifier: • The requirements of this test case are exercised in in FCS_TLSC_EXT.1.2 Test #1 and Test #2. Failed Certificate Path: • Remove the ICA from chain on the TOE. • Attempt the connection from the TOE to the TLS server and verify the connection. • Verify the failure logs on the device. • Verify the **unsuccessful** connection with packet capture. Expired Certificate: • Create a server certificate which is expired. • Show clock on the TOE. • Attempt the connection from the TOE to the TLS server and verify the connection. • Verify the failure logs on the device. • Verify the **unsuccessful** connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects the Invalid certificates. This meets the test requirements.

6.60 FCS_TLSC_EXT.1.3 Test #3

Item	Data
Test ID	FCS_TLSC_EXT.1.3 Test #3
Objective	The purpose of this test to verify that only selected certificate validation failures could be administratively overridden. **If any override mechanism is defined for failed certificate validation**, the evaluator shall configure a new presented certificate that does not contain a valid entry in one of the mandatory fields or parameters (e.g., inappropriate value in extended KeyUsage field) but is otherwise valid and signed by a trusted CA. The evaluator shall confirm that the certificate validation fails (i.e., certificate is rejected), and there is no administrative override available to accept such certificate.
Test Steps	N/A - No override options are available for failed certificate validation
Pass/Fail with Explanation	Pass - No override options are available for failed certificate validation

6.61 FCS_TLSC_EXT.1.4 Test #1

Item	Data
Test ID	FCS_TLSC_EXT.1.4 Test #3
Objective	If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension**, the evaluator shall configure the server to perform ECDHE or DHE (as applicable) key exchange using each of the TOE's supported curves and/or groups. The evaluator shall verify that the TOE successfully connects to the server.

Test Steps & Expected Test Results	• Initiate the connection from the TOE to the TLS Server using the curve secp256r1 and verify the connection. • Verify with packet capture that the required curve is secp256r1. • Initiate the connection from the TOE to the TLS Server using the curve secp384r1 and verify the connection. • Verify with packet capture that the required curve is secp384r1. • Initiate the connection from the TOE to the TLS Server using the curve secp521r1 and verify the connection. • Verify with packet capture that the required curve is secp521r1.
Pass/Fail with Explanation	Pass. The TOE accepted a connection when supported curves were introduced. This meets the test requirements.

6.62 FCS_TLSS_EXT.1.1 Test #1

Item	**Data**
Test ID	FCS_TLSS_EXT.1.1 Test #1
Objective	Test 1: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Steps & Expected Test Results	• Establish a connection with the TOE over TLS using the cipher TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA and verify the connection being successful. • Verify the with packet capture the required ciphersuite is TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA. • Establish a connection with the TOE over TLS using the cipher TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA and verify the connection being successful. • Verify the with packet capture the required ciphersuite is TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA. • Establish a connection with the TOE over TLS using the cipher TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 and verify the connection being successful. • Verify the with packet capture the required ciphersuite is TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. • Establish a connection with the TOE over TLS using the cipher TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 and verify the connection being successful. • Verify the with packet capture the required ciphersuite is TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384. • Establish a connection with the TOE over TLS using the cipher TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and verify the connection being successful. • Verify the with packet capture the required ciphersuite is TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256.

	• Establish a connection with the TOE over TLS using the cipher TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and verify the connection being successful. • Verify the with packet capture the required ciphersuite is TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.
Pass/Fail with Explanation	Pass. The TOE was able to make each connection via the supported ciphersuite. This meets the test requirements.

6.63 FCS_TLSS_EXT.1.1 Test #2

Item	**Data**
Test ID	FCS_TLSS_EXT.1.1 Test #2
Objective	Test 2: The evaluator shall send a Client Hello to the server with a list of ciphersuites that does not contain any of the ciphersuites in the server's ST and verify that the server denies the connection. Additionally, the evaluator shall send a Client Hello to the server containing only the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the server denies the connection.
Test Steps & Expected Test Results	Unsupported ciphersuites in Client Hello: • Attempt to establish a TLS connection to the TOE using the following ciphersuites in the Client Hello: - i. TLS_RSA_WITH_AES_128_CBC_SHA ii. TLS_RSA_WITH_AES_256_CBC_SHA iii. TLS_RSA_WITH_AES_128_CBC_SHA256 • Verify the connection failure via logs on the device for all ciphersuites. • Verify the connection failure via packet capture for all ciphersuites. TLS_NULL_WITH_NULL_NULL only in Client Hello: • Attempt the connection with Acumen-TLS TLSS tool using cipher "TLS_NULL_WITH_NULL_NULL". • Verify the connection failure via logs on the device. • Verify the unsuccessful connection via packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects TLS connections with the non-supported ciphersuites. This meets the testing requirement.

6.64 FCS_TLSS_EXT.1.1 Test #3a

Item	**Data**
Test ID	FCS_TLSS_EXT.1.1 Test #3a
Objective	Modify a byte in the Client Finished handshake message and verify that the server rejects the connection and does not send any application data.
Test Steps & Expected Test Results	• Run the Acumen-TLS TLSS tool with a modified client finished message and wait for the connection, the connection should fail. • Verify the failure logs on the device. • Verify the unsuccessful connection via packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects the connection after receiving the modified Client Handshake message. This meets the test requirements.

6.65 FCS_TLSS_EXT.1.1 Test #3b

Item	**Data**

Test ID	FCS_TLSS_EXT.1.1 Test #3b
Objective	(Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to a) Correctly encrypt (D)TLS Finished message and b) Encrypt every (D)TLS message after session keys is negotiated.) The evaluator shall use one of the claimed ciphersuites to complete a successful handshake and observe transmission of properly encrypted application data. The evaluator shall verify that no Alert with alert level Fatal (2) messages were sent. The evaluator shall verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message. The evaluator shall examine the Finished message (encrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 11 22 33 44 55...) and confirm that it does not contain unencrypted data (unencrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 14 00 00 0c...), by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages. There is a chance that an encrypted Finished message contains a hexadecimal value of '14' at the position where a plaintext Finished message would contain the message type code '14'. If the observed Finished message contains a hexadecimal value of '14' at the position where the plaintext Finished message would contain the message type code, the test shall be repeated three times in total. In case the value of '14' can be observed in all three tests it can be assumed that the Finished message has indeed been sent in plaintext and the test has to be regarded as 'failed'. Otherwise, it has to be assumed that the observation of the value '14' has been due to chance and that the Finished message has indeed been sent encrypted. In that latter case the test shall be regarded as 'passed'.
Test Steps & Expected Test Results	• Initiate a connection to the TOE via Acumen-tlss from the evaluator machine. • Verify that no Alert with alert level Fatal (2) messages were sent. Verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message. • Examine the Finished message and confirm that it does not contain unencrypted data by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages.
Pass/Fail with Explanation	Pass. The Finished message contains Hexadecimal 16 and is sent immediately after Hexadecimal 14 in the ChangeCipherSpec message. The first byte of the encrypted Finished message does not equal hexadecimal 14. This meets the testing requirement.

6.66 FCS_TLSS_EXT.1.2 Test #1

Item	**Data**
Test ID	FCS_TLSS_EXT.1.2 Test #1
Objective	The evaluator shall send a Client Hello requesting a connection for all mandatory and selected protocol versions in the SFR (e.g., by enumeration of protocol versions in a test client) and verify that the server denies the connection for each attempt.

Test Steps & Expected Test Results	• Initiate a connection with the TOE over TLS using the SSLv2.0 and show the connection being unsuccessful. • Verify the connection failure via logs on the device. • Verify the connection failure via packet capture. • Initiate a connection with the TOE over TLS using the SSLv3.0 and show the connection being unsuccessful. • Verify the connection failure via logs on the device. • Verify the connection failure via packet capture. • Initiate a connection with the TOE over TLS using the TLSv1.0 and showing the connection being unsuccessful. • Verify the connection failure via logs on the device. • Verify the connection failure via packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects all non-TLS v1.1 and TLS v1.2 connection attempts. This meets the testing requirement.

6.67 FCS_TLSS_EXT.1.3 Test #1a

Item	**Data**
Test ID	FCS_TLSS_EXT.1.3 Test #1a
Objective	If **ECDHE ciphersuites** are supported: The evaluator shall repeat this test for each supported elliptic curve. The evaluator shall attempt a connection via a supported ECDHE ciphersuite and a single supported elliptic curve specified in the Elliptic Curves Extension. The Evaluator shall verify (though a packet capture or instrumented client) that the TOE selects the same curve in the Server Key Exchange message and successfully establishes the connection.
Test Steps & Expected Test Results	• Initiate a connection with the TOE over TLS using the curve secp256r1 and verify the connection being successful. • Verify the packet capture for successful connection. • Initiate a connection with the TOE over TLS using the curve secp384r1 and verify the connection being successful. • Verify the packet capture for successful connection. • Initiate a connection with the TOE over TLS using the curve secp521r1 and verify the connection being successful. • Verify the packet capture for successful connection.
Pass/Fail with Explanation	Pass. The TOE was able to make connection using each supported elliptic curve. This meets the test requirements.

6.68 FCS_TLSS_EXT.1.3 Test #1b

Item	**Data**
Test ID	FCS_TLSS_EXT.1.3 Test #1b
Objective	If **ECDHE ciphersuites** are supported: The evaluator shall attempt a connection via a supported ECDHE ciphersuite and a single unsupported elliptic curve (e.g., secp192r1 (0x13)) specified in RFC4492, chap. 5.1.1. The evaluator shall verify that the TOE does not send a Server Hello message and the connection is not successfully established.
Test Steps & Expected Test Results	• Initiate a connection with the TOE over TLS using the supported ciphersuite and unsupported elliptical curve and verify the connection fails. • Verify the failure logs on the device.

	- Verify the unsuccessful connection via packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects a connection with unsupported curves. This meets the testing requirements.

6.69 FCS_TLSS_EXT.1.4 Test #1

Item	**Data**
Test ID	FCS_TLSS_EXT.1.4 Test #1
Objective	If the **TOE does not support session resumption based on session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2) or session tickets according to RFC5077**, the evaluator shall perform the following test: a) The client sends a Client Hello with a zero-length session identifier and with a SessionTicket extension containing a zero-length ticket. b) The client verifies the server does not send a NewSessionTicket handshake message (at any point in the handshake). c) The client verifies the Server Hello message contains a zero-length session identifier or passes the following steps: Note: The following steps are only performed if the ServerHello message contains a non-zero length SessionID. d) The client completes the TLS handshake and captures the SessionID from the ServerHello. e) The client sends a ClientHello containing the SessionID captured in step d). This can be done by keeping the TLS session in step d) open or start a new TLS session via the SessionID captured in step d). f) The client verifies the TOE: a. implicitly rejects the SessionID by sending a ServerHello containing a different SessionID and by performing a full handshake (as shown in Figure 1 of RFC 4346 or RFC 5246), or b. terminates the connection in some way that prevents the flow of application data. Remark: If multiple contexts are supported for session resumption, the session ID or session ticket may be obtained in one context for resumption in another context. It is possible that one or more contexts may only permit the construction of sessions to be reused in other contexts but not actually permit resumption themselves. For contexts which do not permit resumption, the evaluator is required to verify this behaviour subject to the description provided in the TSS. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session. **[TD0569 Applied]**
Test Steps & Expected Test Results	- Use the Acumen-TLS TLSS tool to initiate a connection to the TOE and verify TOE doesn't set a session ID or ticket. - Verify with the packet capture that the TOE does not set a session ID or ticket.
Pass/Fail with Explanation	Pass. TOE does not support session resumption based on session IDs or session ticket. This meets the testing requirements.

6.70 FPT_TST_EXT.1 Test #1

Item	**Data**

Test ID	FPT_TST_EXT.1 Test #1
Objective	It is expected that at least the following tests are performed: a) Verification of the integrity of the firmware and executable software of the TOE b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs. The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this. For distributed TOEs the evaluator shall perform testing of self-tests on all TOE components according to the description in the TSS about which self-test are performed by which component.
Test Steps & Expected Test Results	• Power on the TOE and observer the TOE Start up. • Ensure that evidence of the execution of self-tests are provided.
Pass/Fail with Explanation	Pass. The TOE successfully executes self-test. This meets the testing requirement.

6.71 FPT_TUD_EXT.1 Test #1

Item	**Data**
Test ID	FPT_TUD_EXT.1 Test #1
Objective	The evaluator performs the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating). The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE. (For some TOEs loading the update onto the TOE and activation of the update are separate steps (‘activation’ could be performed e.g., by a distinct activation step or by rebooting the device). In that case the evaluator verifies after loading the update onto the TOE but before activation of the update that the current version of the product did not change but the most recently installed version has changed to the new product version.) After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and most recently installed version match again.
Test Steps & Expected Test Results	• Verify the current version of the TOE. • Click on Update Software file and upload the image on the TOE. • Click on Verification file and upload the checksum file on the TOE. • Boot the uploaded image and wait for some time until the booting is done. • After reboot, show new version of software. • Verify the installation via logs.
Pass/Fail with Explanation	Pass. The TOE can be successfully updated. This meets the testing requirements.

6.72 FPT_TUD_EXT.1 Test #2 (a)

Item	**Data**
Test ID	FPT_TUD_EXT.1 Test #2 (a)
Objective	Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted).

	The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 1) A modified version (e.g., using a hex editor) of a legitimately signed update If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version, and most recently installed version, reflect the same version information as prior to the update attempt.
Test Steps & Expected Test Results	• Using a Hex editor modify an otherwise good firmware image. • Verify the current firmware version on the TOE. • Upload the modified image on the TOE. • Attempt to install the modified update image and verify that it fails. • Verify the failure with logs. • Verify that version has not changed.
Pass/Fail with Explanation	Pass. The TOE software was able to detect when an image was corrupted and rejected the image. This meets the testing requirements.

6.73 FPT_TUD_EXT.1 Test #2 (b)

Item	**Data**
Test ID	FPT_TUD_EXT.1 Test #2 (b)
Objective	[conditional]: If **the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE** the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 2) An image that has not been signed If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version, and most recently installed version, reflect the same version information as prior to the update attempt.

Test Steps & Expected Test Results	- Verify the current version of the TOE. - Attempt to install an update without a signature. - Verify the TOE rejects the update. - Verify that version has not changed.
Pass/Fail with Explanation	Pass. The TOE software was able to detect when an image was not signed and rejected the image. This meets the testing requirements.

6.74 FPT_TUD_EXT.1 Test #2 (c)

Item	**Data**
Test ID	FPT_TUD_EXT.1 Test #2 (c)
Objective	[conditional]: If **the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE** the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The 5evaluator obtains or produces illegitimate updates as defined below and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 3) An image signed with an invalid signature (e.g., by using a different key as expected for creating the signature or by manual modification of a legitimate signature) If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version, and most recently installed version, reflect the same version information as prior to the update attempt.
Test Steps & Expected Test Results	- Verify the current version of the TOE. - Attempt to install an update with a different signature xml file. - Verify the TOE rejects the update. - Verify the error via logs. - Verify that version has not changed..
Pass/Fail with Explanation	Pass. The TOE software was able to detect when an image had an invalid signature and rejected the image. This meets the testing requirements.

6.75 FIA_X509_EXT.1.1/Rev Test #1a

Item	**Data**
Test ID	FIA_X509_EXT.1.1/Rev Test #1a
Objective	Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and shall use this chain to demonstrate that the function succeeds. Test 1a shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one intermediate CA certificate needs to be provided, together with the leaf certificate from

	outside the TOE, to complete the chain (e.g., by storing only the root CA certificate in the trust store).
Test Steps & Expected Test Results	• Configure TOE to connect to the TLS server. • Create a full chain of certificates to connect to the TOE. • Upload a complete certificate validation chain to the TOE. • Attempt the connection from the TOE to the TLS server. • Verify the successful connection from logs on the device. • Verify the connection is successful via packet capture.
Pass/Fail with Explanation	Pass. When a complete certificate trust chain is present, the TOE can make a successful connection. This meets the test requirements.

6.76 FIA_X509_EXT.1.1/Rev Test #1b

Item	**Data**
Test ID	FIA_X509_EXT.1.1/Rev Test #1b
Objective	Test 1b: The evaluator shall then 'break' the chain used in Test 1a by either removing the trust anchor in the TOE's trust store used to terminate the chain, or by removing one of the intermediate CA certificates (provided together with the leaf certificate in Test 1a) to complete the chain. The evaluator shall show that an attempt to validate this broken chain fails.
Test Steps & Expected Test Results	• Remove the ICA from chain on the TOE. • Attempt the connection from the TOE to the TLS server. • Verify the unsuccessful connection from logs on the device. • Verify the unsuccessful connection via packet capture.
Pass/Fail with Explanation	When an incomplete certificate trust chain is present, the TOE rejects the connection. This meets the test requirements.
Result	Pass

6.77 FIA_X509_EXT.1.1/Rev Test #2

Item	**Data**
Test ID	FIA_X509_EXT.1.1/Rev Test #2
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Test Steps & Expected Test Results	• Create a server certificate which is expired. • Show clock on the TOE. • Attempt the connection from the TOE to the TLS server with an expired certificate. • Verify the error logs on the device. • Verify the connection is unsuccessful via packet capture.
Pass/Fail with Explanation	Pass. A connection including an expired certificate was rejected. This meets the test requirements.

6.78 FIA_X509_EXT.1.1/Rev Test #3

Item	**Data**

Test ID	FIA_X509_EXT.1.1/Rev Test #3
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 3: The evaluator shall test that the TOE can properly handle revoked certificates-–conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the peer certificate and revocation of the peer intermediate CA certificate i.e., the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails. Revocation checking is only applied to certificates that are not designated as trust anchors. Therefore, the revoked certificate(s) used for testing shall not be a trust anchor.
Test Steps & Expected Test Results	1. Valid Certificate: • Create certificates with OCSP EKU and configure URI of the OCSP responder. • Load the root CA on the TOE. • Configure the TOE for OCSP checking. • Configure the TOE for syslog server. • Start OCSP responder for ICA and Server certificates. • Start the Syslog server using Server and ICA certificates. • Verify the successful connection via logs on the TOE. • Verify the successful connection with packet capture. 2. Invalid End Entity Certificate: • Revoke the End Entity certificate. • Start OCSP responder for ICA and Server certificates. • Start the Syslog server using Server and ICA certificates. • Verify the unsuccessful connection via logs on the TOE. • Verify the unsuccessful connection with packet capture. 3. Invalid Intermediate CA Certificate: • Reset the certificate chain and revoke only the intermediate CA certificate. • Start OCSP responder for ICA and Server certificates. • Start the Syslog server using Server and ICA certificates. • Verify the unsuccessful connection via logs on the TOE. Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. Connection with revoked certificates is not accepted by the TOE which meet the requirement.

6.79 FIA_X509_EXT.1.1/Rev Test #4

Item	**Data**
Test ID	FIA_X509_EXT.1.1/Rev Test #4
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.

	If OCSP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set and verify that validation of the CRL fails.
Test Steps & Expected Test Results	• Generate a certificate that does NOT have OCSP signing purpose. • Use this certificate in the OCSP responder. • Attempt the connection from the TOE to the TLS server and verify the connection being unsuccessful. • Verify the unsuccessful connection logs on the device. • Verify the unsuccessful connection via packet capture.
Pass/Fail with Explanation	Pass. The TOE does not connect to the TLS and OCSP servers if OCSP signing is missing.

6.80 FIA_X509_EXT.1.1/Rev Test #5

Item	**Data**
Test ID	FIA_X509_EXT.1.1/Rev Test #5
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Test Steps & Expected Test Results	• Run the Acumen-TLS TLSC tool with modified byte within the first 8 bytes of the certificate, the connection should fail. • Verify the error with logs on the TOE. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. TOE rejects connections when the first 8 bytes of the certificate are modified. This meets the test requirements.

6.81 FIA_X509_EXT.1.1/Rev Test #6

Item	**Data**
Test ID	FIA_X509_EXT.1.1/Rev Test #6
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the certificate signatureValue field (see RFC5280 Sec. 4.1.1.3), which is normally the last field in the certificate, and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Steps & Expected Test Results	• Run the Acumen-TLSC tool with modified last byte of the certificate. • Verify the error with logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects connections when the last byte of the certificate is modified. This meets the test requirements.

6.82 FIA_X509_EXT.1.1/Rev Test #7

Item	Data
Test ID	FIA_X509_EXT.1.1/Rev Test #7
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.)
Test Steps & Expected Test Results	• Run the Acumen-TLSC tool with modified public key in the certificate. • Verify the error with logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects connections when the public key of the certificate is modified. This meets the test requirements.

6.83 FIA_X509_EXT.1.1/Rev Test #8a

Item	Data
Test ID	FIA_X509_EXT.1.1/Rev Test #8a
Objective	Test 8: (Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen). The evaluator shall establish a valid, Test 8a: (Conditional on TOE ability to process CA certificates presented in certificate message) The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g., by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a valid chain of EC certificates (terminating in a trusted CA certificate), where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain. **TD0527 has been applied**
Test Steps & Expected Test Results	• Configure the EC root CA certificate. • Configure the EC intermediate CA certificate. • Configure the EC node certificate. • Configure the TOE for the root certificate as trust anchor. • Concatenate the CA certificates. • Attempt the connection from the TOE to the TLS server. • Verify the successful connection with packet capture.
Pass/Fail with Explanation	Pass. The evaluator verified the trusted chain of the EC leaf certificate, EC intermediate certificate and EC root certificate and observed that the connection was successful. This meets the test requirements.

6.84 FIA_X509_EXT.1.1/Rev Test #8b

Item	Data
Test ID	FIA_X509_EXT.1.1/Rev Test #8b
Objective	Test 8: (Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen). The evaluator shall establish a valid,

	Test 8b: (Conditional on TOE ability to process CA certificates presented in certificate message) The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g., by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a chain of EC certificates (terminating in a trusted CA certificate), where the intermediate certificate in the certificate chain uses an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid. **TD0527 has been applied**
Test Steps & Expected Test Results	• In the Second part of the test Intermediate certificate is modified with a named curve with an explicit format in the public key information field and is loaded on the TLS server. • Add the modified certificate to the certificate chain. • Concatenate the CA certificates. • Configure the TOE for the root certificate as trust anchor. • Attempt the connection from the TOE to the TLS Server. • Verify the failure logs on the device. • Verify the unsuccessful connection via packet capture.
Pass/Fail with Explanation	Pass. The evaluator verified that when the public key information is modified in the intermediate certificate on the TLS server, TOE is unable to make the successful connection. This meets the test requirements.

6.85 FIA_X509_EXT.1.1/Rev Test #8c

Item	**Data**
Test ID	FIA_X509_EXT.1.1/Rev Test #8c
Objective	Test 8: (Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen). The evaluator shall establish a valid, Test 8c: The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store. **TD0527 has been applied**
Test Steps & Expected Test Results	• In the Third part of the test Intermediate certificate is modified with a named curve with an explicit format in the public key information field and is loaded on the TOE. • Attempt to add the modified Intermediate certificate on the TOE. • Verify that the TOE discards the certificate (But the TOE accepts the certificate).
Pass/Fail with Explanation	Pass. The evaluator verified that when the public key information is modified in the intermediate certificate and is loaded to the TOE’s trust store, TOE does not accept such certificate. This meets the testing requirements.

6.86 FIA_X509_EXT.1.2/Rev Test #1

Item	**Data**

Test ID	FIA_X509_EXT.1.1/Rev Test #1
Objective	The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e., where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted. The goal of the following tests is to verify that the TOE accepts a certificate as a CA certificate only if it has been marked as a CA certificate by using basicConstraints with the CA flag set to True (and implicitly tests that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation). For each of the following tests the evaluator shall create a chain of at least three certificates: - a self-signed root CA certificate, - an intermediate CA certificate and - a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: *(i) as part of the validation of the leaf certificate belonging to this chain.* *(ii) when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e., when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).*
Test Steps & Expected Test Results	• Configure the CA certificate lacking the basicConstraints extension. • Load the certificate lacking the basicConstraints on the TLS server. • Add the modified certificate to the certificate chain. • Concatenate the CA certificates. • Attempt the connection from the TOE to the TLS Server. • Verify the error in logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects certificates signed by a CA that does not contain the basicConstraints extension. This meets the test requirements.

6.87 FIA_X509_EXT.1.2/Rev Test #2

Item	Data
Test ID	FIA_X509_EXT.1.1/Rev Test #2
Objective	The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e., where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted. The goal of the following tests it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation). For each of the following tests the evaluator shall create a chain of at least three certificates:

	- a self-signed root CA certificate, - an intermediate CA certificate and - a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: 1. As part of the validation of the leaf certificate belonging to this chain. 2. When attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e., when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).
Test Steps & Expected Test Results	• Configure the CA certificate with the flag in the basicConstraints extension set to FALSE. • Add the modified certificate to the certificate chain. • Concatenate the CA certificates. • Attempt the connection from the TOE to the TLS Server. • Verify the error in logs on the device. • Verify the unsuccessful connection packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects certificates signed by a CA that has the CA flag in the basicConstraints extension set to FALSE. This meets the test requirements.

6.88 FIA_X509_EXT.2 Test #1

Item	**Data**
Test ID	FIA_X509_EXT.2 Test #2
Objective	The evaluator shall perform the following test for each trusted channel: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the guidance documentation to determine that all supported administrator-configurable options behave in their documented manner.
Test Steps & Expected Test Results	1. Valid Certificate: • Configure the node certificate which is valid and not revoked. • Configure the node certificate showing the OCSP distribution point. • Attempt the connection from the TOE to the TLS server and show the connection being successful. • Attempt the connection from the TOE to the OCSP server and show the connection being successful. • Verify the packet capture between the TOE and the OCSP server. • Verify the packet capture between the TOE and the TLS server. 2. Invalid Certificate: In the Second part of the test node certificate is revoked and the OCSP server is unreachable, TOE does not make the successful connection with the TLS server with the revoked certificate when failed to validate the certificate. • Configure the node certificate which is been revoked. • Configure the node certificate showing the OCSP distribution point.

	• Manipulate the Environment so that TOE is unable to validate the certificate from the OCSP server. • Attempt the connection from the TOE to the TLS server and show the connection being unsuccessful (but it is successful). • Verify the packet capture between the TOE and the TLS server. 3. With administrator-configurable option: In the Third part of the test node certificate is revoked and the OCSP server is unreachable, and TOE is configured to allow the access on OCSP server failure, TOE makes the successful connection with the TLS server with the revoked certificate when failed to validate the certificate. • Configure the node certificate which is been revoked. • Configure the node certificate showing the OCSP distribution point. • Manipulate the Environment so that TOE is unable to validate the certificate from the OCSP server. • Configure the option "Allow Access on Server Failure" on TOE. • Attempt the connection from the TOE to the TLS server and show the connection being successful. • Verify the packet capture between the TOE and the TLS server.
Pass/Fail with Explanation	Inconclusive. When attempted invalid certificate the TOE accepts TLS connection. This does not meet testing requirements.

6.89 FIA_X509_EXT.3 Test #1

Item	**Data**
Test ID	FIA_X509_EXT.3 Test #2
Objective	The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated message and ensure that it conforms to the format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information.
Test Steps & Expected Test Results	• On the TOE, generate a CSR. • Examine the CSR contents on Openssl server.
Pass/Fail with Explanation	Pass. The TOE can generate a CSR with all the requisite information. This meets the test requirements.

6.90 FIA_X509_EXT.3 Test #2

Item	**Data**
Test ID	FIA_X509_EXT.3 Test #2
Objective	The evaluator shall demonstrate that validating a response message to a Certification Request without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the certificate response message and demonstrate that the function succeeds.
Test Steps & Expected Test Results	• Generate a CSR (Certificate Signing Request) on the TOE. • Generate a signed certificate based on the generated CSR from an external CA. • Ensure that the full trust chain for the signed CA is not present on the TOE. • Attempt to load the signed certificate on the TOE.

	• Verify that the option to choose the certificate is disable i.e., it is grayed out and cannot be selected as the full trust chain of the CA is not present. • Add the intermediate certificate to the TOE certificate store to ensure that the TOE has a full certificate path. • Verify from the logs that intermediate certificate is installed. • Verify that the option to choose the certificate is now enable i.e., not grayed out and can be selected since the full trust chain of the CA is present on the TOE. • Verify that the certificate can be used via logs.
Pass/Fail with Explanation	Pass. Evaluator verified that when the certificate raised with CSR is loaded without complete CA chain TOE rejects the certificate and when the complete chain is present TOE accepts the certificate. This meets the testing requirements.

7 Security Assurance Requirements

7.1 ADV_FSP.1 Basic Functional Specification

7.1.1 ADV_FSP.1

7.1.1.1 ADV_FSP.1 Activity 1

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it describes the purpose and method of use for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the purpose and method of use for each security relevant TSFI by verifying the AGD satisfies all the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.2 ADV_FSP.1 Activity 2

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD. Each Guidance Evaluation Activity is associated with a specific SFR. The Evaluation Findings for each Guidance Evaluation Activity identify the relevant interfaces, thus providing a mapping. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.3 ADV_FSP.1 Activity 3

Objective	The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it identifies and describes the parameters for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the parameters for each security relevant TSFI by verifying the AGD satisfies all the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2 AGD_OPE.1 Operational User Guidance

7.2.1 AGD_OPE.1

7.2.1.1 AGD_OPE.1 Activity 1

Objective	The evaluator shall ensure the Operational guidance documentation is distributed to Security Administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that Security Administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.

Evaluator Findings	The evaluator checked the requirements below are met by the guidance documentation. Guidance documentation will be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on www.niap-ccevs.org.. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.2 AGD_OPE.1 Activity 2

Objective	The evaluator shall ensure that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.
Evaluator Findings	The evaluator examined the section titled **Supported Platforms** of the AGD and it was used to determine the verdict of this assurance activity. The ST claims LoadMaster X15, LoadMaster X25, LoadMaster X40 and virtual LoadMaster platforms, and the operational guidance documents cover the configuration and use of these platforms. An additional VMware platform installation document is available from the Kemp website for Virtual LoadMaster installation prerequisites and steps. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.3 AGD_OPE.1 Activity 3

Objective	The evaluator shall ensure that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.
Evaluator Findings	The evaluator ensured that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. While performing the Guidance Evaluation Activities for the cryptographic SFRs, the evaluator ensured guidance contained the necessary instructions for configuring the cryptographic engines. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.4 AGD_OPE.1 Activity 4

Objective	The evaluator shall ensure the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.
Evaluator Findings	The entire AGD was used to determine the verdict of this work unit. Each confirmation command indicates tested options. Additionally, the section titled **Operational Environment** specifies features that are not assessed and tested by the EAs. The evaluator ensured the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

7.2.1.5 AGD_OPE.1 Activity 5 **[TD0536]**

Objective	In addition, the evaluator shall ensure that the following requirements are also met. a) The guidance documentation shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. b) The documentation must describe the process for verifying updates to the TOE for each method selected for FPT_TUD_EXT.1.3 in the Security Target. The evaluator shall verify that this process includes the following steps: i) Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory). ii) Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes instructions that describe at least one method of validating the hash/digital signature. c) The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The guidance documentation shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.
Evaluator Findings	The evaluator verified the guidance documentation contains instructions for configuring any cryptographic engines in AGD_OPE.1 Test #3. The evaluator verified the guidance documentation describes the process for verifying updates in FPT_TUD_EXT.1 Guidance 2. The evaluator verified the guidance documentation makes it clear which security functionality is covered by the Evaluation Activities in AGD_OPE.1 Test #4. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3 AGD_PRE.1 Preparative Procedures

7.3.1 AGD_PRE.1

7.3.1.1 AGD_PRE.1 Activity 1

Objective	The evaluator shall examine the Preparative procedures to ensure they include a description of how the Security Administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target).
Evaluator Findings	The evaluator examined the Preparative procedures to ensure they include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality. The evaluator reviewed the sections titled **Operational Environment** of the AGD. The evaluator found that these sections describe how the Operational Environment must meet: • Management Workstation • Audit Server • ESXi Server • LDAP Server

	• NTP Server Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.2 AGD_PRE.1 Activity 2

<table>
<tr><td>Objective</td><td>The evaluator shall examine the Preparative procedures to ensure they are provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.</td></tr>
<tr><td>Evaluator Findings</td><td>The evaluator checked the preparative procedures to ensure that they include a description of how the operational environment can fulfill its role to support the TSF. Section titled ‘Operational Environment’ of the AGD was used to determine the verdict of this assurance activity. The AGD describes each environmental component and its role as necessary to support the TOE functionality, as follows:
<table>
<tr><th>Component</th><th>Usage/Purpose Description</th></tr>
<tr><td>Management Workstation</td><td>Workstation providing local console access to the TOE.
Workstation providing a browser to connected to the Web User Interface (WUI) over TLSv1.2 or TLSv1.1.</td></tr>
<tr><td>Audit Server</td><td>Syslog server that receives audit logs from the TOE over TLSv1.2 or TLSv1.1.</td></tr>
<tr><td>ESXi Server</td><td>ESXi v6.7 acting as the hypervisor for Virtual LoadMaster.</td></tr>
<tr><td>LDAP Server</td><td>Optional authentication server supporting LDAP over TLSv1.2 or TLSv1.1.</td></tr>
<tr><td>NTP Server</td><td>Optional NTP server supporting SHA-1 integrity verification.</td></tr>
</table>
Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

7.3.1.3 AGD_PRE.1 Activity 3

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.
Evaluator Findings	The evaluator checked the requirements are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AGD describes all of the functions necessary to install and configure the TOE to work in the target operating environment, including, • Configuring Administrative Accounts and Passwords • Configuring Console Connections • Configuring the Remote Syslog Server • Configuring Audit Log Options • Configuring Event Logging • Configuring a Secure Logging Channel • Configuring NTP server • Generating CSR • Configuring certificates

	- Configuring Idle session Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.4 AGD_PRE.1 Activity 4

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to manage the security of the TSF as a product and as a component of the larger operational environment.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. The entire AGD was used to determine the verdict of this work unit. The same commands, configurations, and interfaces used to install the TOE are also used for ongoing management, so this is satisfied by AGD_PRE.1 Test #3. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.5 AGD_PRE.1 Activity 5

Objective	In addition, the evaluator shall ensure that the following requirements are also met. The preparative procedures must a) include instructions to provide a protected administrative capability; and b) identify TOE passwords that have default values associated with them and instructions shall be provided for how these can be changed.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability and changing default passwords. The sections titled CC Configuration Process were used to determine the verdict of this work unit. The AGD describes changing the default password associated with the root account and configuring SSH for remote administration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4 ALC Assurance Activities

7.4.1 ALC_CMC.1

7.4.1.1 ALC_CMC.1 Activity 1

Objective	When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

7.4.2 ALC_CMS.1

7.4.2.1 ALC_CMS.1 Activity 1

Objective	When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. If required TOE model or version is not available then Kemp support should be reached out. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.5 ATE_IND.1 Independent Testing – Conformance

7.5.1 ATE_IND.1

7.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator performs the CEM work units associated with the ATE_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4. The evaluator should consult Appendix 709 when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.
Evaluator Findings	The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6 AVA_VAN.1 Vulnerability Survey

7.6.1 AVA_VAN.1

7.6.1.1 AVA_VAN.1 Activity 1 **[TD0564, Labgram #116]**

Objective	The evaluator shall document their analysis and testing of potential vulnerabilities with respect to this requirement.
Evaluator Findings	The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE

	software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below. • https://nvd.nist.gov/view/vuln.search • http://cve.mitre.org/cve • https://www.cvedetails.com/vulnerability-search.php • https://www.kb.cert.org/vuls/search/ • www.exploitsearch.net • www.securiteam.com • http://nessus.org/plugins/index.php?view=search • http://www.zerodayinitiative.com/advisories • https://www.exploit-db.com • https://www.rapid7.com/db/vulnerabilities The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on January 13, 2023. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. The list of keywords searched include: • Kemp Loadmaster v7.2 • LoadMaster FIPS Object Module v1.0 • Load Balancer • Intel Xeon E3-1275v6 • Intel Xeon E5-4620v4 • Openssl v1.1.1n • freeradius-client • Libmcrypt v 2.5.7 • Openldap v2.4.32 • openssl-fips • syslog ng v3.25.1 The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.2 AVA_VAN.1 Activity 2

Objective	The evaluator shall perform the following activities to generate type 4 flaw hypotheses: • Fuzz testing ○ Examine effects of sending: ▪ mutated packets carrying each ‘Type’ and ‘Code’ value that is undefined in the relevant RFC for each of ICMPv4 (RFC 792) and ICMPv6 (RFC 4443) ▪ mutated packets carrying each ‘Transport Layer Protocol’ value that is undefined in the respective RFC for IPv4 (RFC 791) IPv6 (RFC 2460) should also be covered if it is supported and claimed by the TOE.

	Since none of these packets will belong to an allowed session, the packets should not be processed by the TOE, and the TOE should not be adversely affected by this traffic. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis. ○ Mutation fuzz testing of the remaining fields in the required protocol headers. This testing requires sending mutations of well- formed packets that have both carefully chosen and random values inserted into each header field in turn (i.e., testing is to include both carefully chosen and random insertion test cases). The original well-formed packets would be accepted as part of a normal existing communication stream and may still be accepted as valid packets when subject to the carefully chosen mutations (the individual packet alone would be valid although its contents may not be valid in the context of preceding and/or following packets) but will often not be valid packets when random values are inserted into fields. The carefully chosen values should include semantically significant values that can be determined from the type of the data that the field represents, such as values indicating positive and negative integers, boundary conditions, invalid binary combinations (e.g., for flag sets with dependencies between bits), and missing start or end values. Randomly chosen values may not result in well-formed packets but are included nonetheless to see whether they can lead to the device entering an insecure state. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.
Evaluator Findings	The evaluator documented the fuzz testing results with respect to this requirement. The evaluation lab examined each result from fuzz testing to determine if the TOE improperly processes packets. Based upon the analysis, no unexpected results occurred. Therefore, no Type 4 hypotheses were generated. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

8 Conclusion

The testing shows that all test cases required for conformance have passed testing.

End of Document