

**Assurance Activity Report for  
Cisco 8000 Series Routers running IOS-XR Version 7.3**

Security Target Name

Cisco 8000 Series Routers running IOS-XR Version 7.3 Security Target

**collaborative Protection Profile for Network Devices  
Version 2.2e**

AAR Version 0.3

**Evaluated by:**



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:**

Cisco Systems, Inc.

### **The Author of the Security Target:**

Cisco Systems, Inc.

### **The TOE Evaluation was Sponsored by:**

Cisco Systems, Inc.

### **Evaluation Personnel:**

Kamran Farogh

Rahul Joshi

Shaunak Shah

### **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	09/16/2022	Initial Release
0.2	10/24/2022	Updated to address the ECR comments
0.3	11/07/2022	Updated a Table entry in Section 4.3

---

# Contents

- 1 TOE Overview.....18**
  - 1.1 TOE Overview ..... 18
  - 1.2 TOE Description ..... 18
- 2 Assurance Activities Identification.....18**
- 3 Test Equivalency Justification .....18**
  - 3.1 Architectural Description ..... 18
  - 3.2 Specification of Differences..... 19
  - 3.3 Equivalency Analysis ..... 20
  - 3.4 Platform/Hardware Dependencies..... 20
  - 3.5 Software/OS Dependencies: ..... 21
  - 3.6 Differences in Libraries Used to Provide TOE Functionality ..... 21
  - 3.7 TOE Management Interface Differences..... 21
  - 3.8 TOE Functional Differences ..... 21
  - 3.9 Difference Comparison ..... 25
  - 3.10 MACsec Analysis ..... 27
  - 3.11 Conclusions ..... 27
- 4 Test Bed Descriptions .....27**
  - 4.1 Test Bed – Audit, Auth, SSHS, TLSC, Update, X509-Rev ..... 27
  - 4.2 Test Bed – MACsec..... 27
  - 4.3 Labgram ..... 28
- Test Time & Location .....30**
- 5 Detailed Test Cases (TSS and Guidance Activities) .....30**
  - 5.1 TSS and Guidance Activities (Auditing) ..... 30
    - 5.1.1 FAU\_GEN.1 ..... 30
      - 5.1.1.1 FAU\_GEN.1 TSS 1 .....30

5.1.1.2	FAU_GEN.1 Guidance 1 .....	30
5.1.1.3	FAU_GEN.1 Guidance 2 .....	31
5.1.2	FAU_STG_EXT.1 .....	33
5.1.2.1	FAU_STG_EXT.1 TSS 1 .....	33
5.1.2.2	FAU_STG_EXT.1 TSS 2 .....	34
5.1.2.3	FAU_STG_EXT.1 TSS 3 .....	34
5.1.2.4	FAU_STG_EXT.1 TSS 4 .....	35
5.1.2.5	FAU_STG_EXT.1 TSS 5 .....	35
5.1.2.6	FAU_STG_EXT.1 Guidance 1 .....	36
5.1.2.7	FAU_STG_EXT.1 Guidance 2 .....	37
5.1.2.8	FAU_STG_EXT.1 Guidance 3 .....	37
<b>6</b>	<b>TSS and Guidance Activities (Cryptographic Support) .....</b>	<b>38</b>
6.1.1	FCS_CKM.1 .....	38
	FCS_CKM.1 TSS 1 .....	38
	FCS_CKM.1 Guidance 1 .....	39
6.1.2	FCS_CKM.2 .....	40
	FCS_CKM.2 TSS 1 <b>[TD0580]</b> .....	40
	FCS_CKM.2 Guidance 1 .....	41
6.1.3	FCS_CKM.4 .....	42
	FCS_CKM.4 TSS 1 .....	42
	FCS_CKM.4 TSS 2 .....	45
	FCS_CKM.4 TSS 3 .....	46
	FCS_CKM.4 TSS 4 .....	46
	FCS_CKM.4 TSS 5 .....	47
	FCS_CKM.4 Guidance 1 .....	47
6.1.4	FCS_COP.1/DataEncryption .....	48
	FCS_COP.1/DataEncryption TSS 1 .....	48
	FCS_COP.1/DataEncryption Guidance 1 .....	48

	FCS_COP.1/DataEncryption Test/CAVP 1 .....	49
6.1.5	FCS_COP.1/SigGen .....	49
	FCS_COP.1/SigGen TSS 1 .....	49
	FCS_COP.1/SigGen Guidance 1 .....	49
	FCS_COP.1/SigGen Test/CAVP 1 .....	50
6.1.6	FCS_COP.1/Hash .....	50
	FCS_COP.1/Hash TSS 1 .....	50
	FCS_COP.1/Hash Guidance 1 .....	50
	FCS_COP.1/Hash Test/CAVP 1 .....	50
6.1.7	FCS_COP.1/KeyedHash .....	51
	FCS_COP.1/KeyedHash TSS 1 .....	51
	FCS_COP.1/KeyedHash Guidance 1 .....	51
	FCS_COP.1/KeyedHash Test/CAVP 1 .....	52
6.1.8	FCS_COP.1(1)/KeyedHashCMAC .....	52
	FCS_COP.1(1)/KeyedHashCMAC TSS 1 [TD0466] .....	52
6.1.9	FCS_COP.1(5) .....	52
	FCS_COP.1(5) TSS 1 [TD0466] .....	52
6.1.10	FCS_RBG_EXT.1 .....	53
	FCS_RBG_EXT.1 TSS 1 .....	53
	FCS_RBG_EXT.1 Guidance 1 .....	53
	FCS_RBG_EXT.1.1 Test/CAVP 1 .....	53
<b>7</b>	<b>TSS and Guidance Activities (MACsec) .....</b>	<b>54</b>
7.1.1	FCS_MACSEC_EXT.1 .....	54
	FCS_MACSEC_EXT.1 TSS 1 .....	54
	FCS_MACSEC_EXT.1 TSS 2 .....	54
	FCS_MACSEC_EXT.1 TSS 3 [TD0553] .....	55
7.1.2	FCS_MACSEC_EXT.2 .....	55
	FCS_MACSEC_EXT.2 TSS 1 .....	55

	FCS_MACSEC_EXT.2 Guidance 1.....	56
7.1.3	FCS_MACSEC_EXT.3 .....	56
	FCS_MACSEC_EXT.3 TSS 1 .....	56
7.1.4	FCS_MACSEC_EXT.4 .....	57
	FCS_MACSEC_EXT.4 TSS 1 .....	57
	FCS_MACSEC_EXT.4 Guidance 1.....	57
7.1.5	FCS_MKA_EXT.1 .....	58
	FCS_MKA_EXT.1.4 TSS 1 .....	58
	FCS_MKA_EXT.1.8 TSS 1 .....	58
	FCS_MKA_EXT.1.8 TSS 2 .....	59
	FCS_MKA_EXT.1.8 TSS 3 .....	59
	FCS_MKA_EXT.1.8 Guidance 1.....	59
<b>8</b>	<b>TSS and Guidance Activities (SSH) .....</b>	<b>60</b>
8.1.1	FCS_SSHS_EXT.1.....	60
	FCS_SSHS_EXT.1.2 TSS 1 .....	60
	FCS_SSHS_EXT.1.3 TSS 1 .....	61
	FCS_SSHS_EXT.1.4 TSS 1 .....	61
	FCS_SSHS_EXT.1.4 Guidance 1 .....	61
	FCS_SSHS_EXT.1.5 TSS 1 .....	62
	FCS_SSHS_EXT.1.5 Guidance 1 .....	62
	FCS_SSHS_EXT.1.6 TSS 1 .....	62
	FCS_SSHS_EXT.1.6 Guidance 1 .....	63
	FCS_SSHS_EXT.1.7 TSS 1 .....	63
	FCS_SSHS_EXT.1.7 Guidance 1 .....	64
	FCS_SSHS_EXT.1.8 TSS 1 .....	64
	FCS_SSHS_EXT.1.8 Guidance 1 .....	64
<b>9</b>	<b>TSS and Guidance Activities (TLS) .....</b>	<b>65</b>
9.1.1	FCS_TLSC_EXT.1 .....	65

	FCS_TLSC_EXT.1.1 TSS 1 .....	65
	FCS_TLSC_EXT.1.1 Guidance 1 .....	66
	FCS_TLSC_EXT.1.2 TSS 1 .....	66
	FCS_TLSC_EXT.1.2 TSS 2 .....	66
	FCS_TLSC_EXT.1.2 Guidance 1 .....	67
	FCS_TLSC_EXT.1.4 TSS 1 .....	68
	FCS_TLSC_EXT.1.4 Guidance 1 .....	68
<b>10</b>	<b>TSS and Guidance Activities (Identification and Authentication) .....</b>	<b>68</b>
10.1.1	FIA_AFL.1 .....	68
	FIA_AFL.1 TSS 1 .....	68
	FIA_AFL.1 TSS 2 .....	69
	FIA_AFL.1 Guidance 1 .....	69
	FIA_AFL.1 Guidance 2 .....	70
10.1.2	FIA_AFL.1/MACsec .....	70
	FIA_AFL.1/MACsec Guidance 1 .....	70
10.1.3	FIA_PMG_EXT.1 .....	71
	FIA_PMG_EXT.1.1 TSS 1 .....	71
	FIA_PMG_EXT.1.1 Guidance 1 .....	71
10.1.4	FIA_PSK_EXT.1/MACsec .....	72
	FIA_PSK_EXT.1/MACsec TSS 1 .....	72
	FIA_PSK_EXT.1/MACsec Guidance 1 .....	72
	FIA_PSK_EXT.1/MACsec Guidance 2 .....	73
10.1.5	FIA_UIA_EXT.1 .....	73
	FIA_UIA_EXT.1 TSS 1 .....	73
	FIA_UIA_EXT.1 TSS 2 .....	74
	FIA_UIA_EXT.1 Guidance 1 .....	74
10.1.6	FIA_UAU.7 .....	75
	FIA_UAU.7 Guidance 1 .....	75



10.1.7	FIA_X509_EXT.1/Rev .....	75
	FIA_X509_EXT.1/Rev TSS 1 .....	75
	FIA_X509_EXT.1/Rev TSS 2 .....	76
	FIA_X509_EXT.1/Rev Guidance 1 .....	77
10.1.8	FIA_X509_EXT.2 .....	78
	FIA_X509_EXT.2 TSS 1.....	78
	FIA_X509_EXT.2 TSS 2.....	78
	FIA_X509_EXT.2 Guidance 1.....	78
10.1.9	FIA_X509_EXT.3 .....	80
	FIA_X509_EXT.3 TSS 1.....	80
	FIA_X509_EXT.3 Guidance 1.....	80
<b>11</b>	<b>TSS and Guidance Activities (Security Management) .....</b>	<b>83</b>
11.1.1	FMT_MOF.1/ManualUpdate.....	83
	FMT_MOF.1/ManualUpdate Guidance 1 .....	83
11.1.2	FMT_MOF.1/Services.....	84
	FMT_MOF.1/Services TSS 2 .....	84
	FMT_MOF.1/Services Guidance 2.....	84
11.1.3	FMT_MTD.1/CoreData.....	85
	FMT_MTD.1/CoreData TSS 1 .....	85
	FMT_MTD.1/CoreData TSS 2 .....	86
	FMT_MTD.1/CoreData Guidance 1 .....	86
	FMT_MTD.1/CoreData Guidance 2 .....	87
11.1.4	FMT_MTD.1/CryptoKeys.....	89
	FMT_MTD.1/CryptoKeys TSS 2 .....	89
	FMT_MTD.1/CryptoKeys Guidance 2 .....	91
11.1.5	FMT_SMF.1 .....	92
	FMT_SMF.1 TSS 1.....	92
	FMT_SMF.1.1/MACsec TSS 1 [TD0652] .....	94

	FMT_SMF.1/MACsec Guidance 1 .....	95
11.1.6	FMT_SMR.2 .....	97
	FMT_SMR.2 TSS 1 .....	97
	FMT_SMR.2 Guidance 1.....	97
<b>12</b>	<b>TSS and Guidance Activities (Protection of the TSF) .....</b>	<b>98</b>
12.1.1	FPT_APW_EXT.1 .....	98
	FPT_APW_EXT.1 TSS 1 .....	98
12.1.2	FPT_CAK_EXT.1 .....	98
	FPT_CAK_EXT.1 TSS 1.....	98
12.1.3	FPT_FLS.1(2)/SelfTest.....	99
	FPT_FLS.1(2)/SelfTest TSS 1 <b>[TD0190]</b> .....	99
	FPT_FLS.1(2)/SelfTest Guidance 1 <b>[TD0190]</b> .....	99
12.1.4	FPT_RPL.1.....	100
	FPT_RPL.1.2 TSS 1 .....	100
12.1.5	FPT_SKP_EXT.1.....	100
	FPT_SKP_EXT.1 TSS 1 .....	100
12.1.6	FPT_STM_EXT.1.....	101
	FPT_STM_EXT.1 TSS 1.....	101
	FPT_STM_EXT.1 Guidance 1 .....	101
12.1.7	FPT_TST_EXT.1.1 .....	102
	FPT_TST_EXT.1.1 TSS 1 .....	102
	FPT_TST_EXT.1.1 Guidance 1.....	103
12.1.8	FPT_TUD_EXT.1.....	104
	FPT_TUD_EXT.1 TSS 1 .....	104
	FPT_TUD_EXT.1 TSS 2 .....	104
	FPT_TUD_EXT.1 TSS 5 .....	105
	FPT_TUD_EXT.1 Guidance 1 .....	106
	FPT_TUD_EXT.1 Guidance 2 .....	106

	FPT_TUD_EXT.1 Guidance 3 .....	106
	FPT_TUD_EXT.1 Guidance 6 .....	107
<b>13</b>	<b>TSS and Guidance Activities (TOE Access) .....</b>	<b>107</b>
13.1.1	FTA_SSL_EXT.1 .....	107
	FTA_SSL_EXT.1 TSS 1 .....	107
	FTA_SSL_EXT.1 Guidance 1.....	108
13.1.2	FTA_SSL.3 .....	108
	FTA_SSL.3 TSS 1 .....	108
	FTA_SSL.3 Guidance 1.....	108
13.1.3	FTA_SSL.4 .....	109
	FTA_SSL.4 TSS 1 .....	109
	FTA_SSL.4 Guidance 1.....	109
13.1.4	FTA_TAB.1 .....	110
	FTA_TAB.1 TSS 1 .....	110
	FTA_TAB.1 Guidance 1.....	110
<b>14</b>	<b>TSS and Guidance Activities (Trusted Path/Channels) .....</b>	<b>111</b>
14.1.1	FTP_ITC.1.....	111
	FTP_ITC.1 TSS 1.....	111
	FTP_ITC.1 Guidance 1 .....	111
14.1.2	FTP_TRP.1/Admin .....	112
	FTP_TRP.1/Admin TSS 1.....	112
	FTP_TRP.1/Admin Guidance 1 .....	112
<b>15</b>	<b>Detailed Test Cases (Test Activities).....</b>	<b>114</b>
<b>15.1.1</b>	<b>Audit.....</b>	<b>114</b>
	FAU_GEN.1 Test #1.....	114
	FAU_STG_EXT.1 Test #1.....	115
	FAU_STG_EXT.1 Test #2 (b) .....	115
	FAU_STG_EXT.1 Test #3.....	116

FPT_STM_EXT.1 Test #1.....	117
FTP_ITC.1 Test #1.....	117
FTP_ITC.1 Test #2.....	118
FTP_ITC.1 Test #3.....	118
FTP_ITC.1 Test #4.....	118
FTP_ITC.1/MACSEC Test #4 .....	120
<b>15.1.2 Auth.....</b>	<b>120</b>
FCS_CKM.2 RSA.....	120
FCS_CKM.2 FCC.....	121
FIA_AFL.1 Test #1.....	121
FIA_AFL.1 Test #2b .....	122
FIA_PMG_EXT.1 Test #1 .....	123
FIA_PMG_EXT.1 Test #2 .....	124
FIA_UIA_EXT.1 Test #1.....	125
FIA_UIA_EXT.1 Test #2.....	125
FIA_UIA_EXT.1 Test #3.....	126
FIA_UAU.7 Test #1 .....	127
FMT_MOF.1/ManualUpdate Test #1 .....	127
FMT_MOF.1/ManualUpdate Test #2 .....	128
FMT_MOF.1/Services Test #1.....	128
FMT_MOF.1/Services Test #2.....	129
FMT_MTD.1/CryptoKeys Test #1.....	129
FMT_MTD.1/CryptoKeys Test #2.....	130
FMT_SMF.1 Test #1 .....	131
FMT_SMR.2 Test #1 .....	131
FTA_SSL.3 Test #1 .....	131
FTA_SSL.4 Test #1 .....	132

FTA_SSL.4 Test #2 .....	133
FTA_SSL_EXT.1.1 Test #1 .....	133
FTA_TAB.1 Test #1 .....	134
FTP_TRP.1/Admin Test #1 .....	134
FTP_TRP.1/Admin Test #2 .....	135
<b>15.1.3       SSHS.....</b>	<b>136</b>
FCS_SSHS_EXT.1.2 Test #1.....	136
FCS_SSHS_EXT.1.2 Test #2.....	137
FCS_SSHS_EXT.1.2 Test #3.....	137
FCS_SSHS_EXT.1.2 Test #4.....	138
FCS_SSHS_EXT.1.3 Test #1.....	138
FCS_SSHS_EXT.1.4 Test #1.....	139
FCS_SSHS_EXT.1.5 Test #1.....	140
FCS_SSHS_EXT.1.5 Test #2.....	141
FCS_SSHS_EXT.1.6 Test #1.....	141
FCS_SSHS_EXT.1.6 Test #2.....	142
FCS_SSHS_EXT.1.7 Test #1.....	143
FCS_SSHS_EXT.1.7 Test #2.....	144
FCS_SSHS_EXT.1.8 Test #1t .....	144
FCS_SSHS_EXT.1.8 Test #1b.....	145
<b>15.1.4       TLSC .....</b>	<b>147</b>
FCS_TLSC_EXT.1.1 Test #1 .....	147
FCS_TLSC_EXT.1.1 Test #2 .....	148
FCS_TLSC_EXT.1.1 Test #3 .....	148
FCS_TLSC_EXT.1.1 Test #4a .....	149
FCS_TLSC_EXT.1.1 Test #4b .....	149
FCS_TLSC_EXT.1.1 Test #5a .....	150

FCS_TLSC_EXT.1.1 Test #6a .....	150
FCS_TLSC_EXT.1.1 Test #6b .....	151
FCS_TLSC_EXT.1.1 Test #6c .....	151
FCS_TLSC_EXT.1.2 Test #1 .....	152
FCS_TLSC_EXT.1.2 Test #2 .....	153
FCS_TLSC_EXT.1.2 Test #3 .....	154
FCS_TLSC_EXT.1.2 Test #4 .....	155
FCS_TLSC_EXT.1.2 Test #5 (1).....	155
FCS_TLSC_EXT.1.2 Test #5 (2)(a) .....	156
FCS_TLSC_EXT.1.2 Test #5 (2)(b) .....	157
FCS_TLSC_EXT.1.2 Test #5 (2)(c).....	158
FCS_TLSC_EXT.1.3 Test #1 .....	159
FCS_TLSC_EXT.1.3 Test #2 .....	159
FCS_TLSC_EXT.1.3 Test #3 .....	160
<b>15.1.4 Update .....</b>	<b>161</b>
FPT_TST_EXT.1 Test #1 .....	161
FPT_TUD_EXT.1 Test #1.....	161
FPT_TUD_EXT.1 Test #2 (a) .....	162
FPT_TUD_EXT.1 Test #2 (b) .....	163
FPT_TUD_EXT.1 Test #2 (c).....	164
<b>15.1.5 X509-Rev.....</b>	<b>166</b>
FIA_X509_EXT.1.1/Rev Test #1a.....	166
FIA_X509_EXT.1.1/Rev Test #1b.....	166
FIA_X509_EXT.1.1/Rev Test #2.....	167
FIA_X509_EXT.1.1/Rev Test #3.....	168
FIA_X509_EXT.1.1/Rev Test #4.....	169
FIA_X509_EXT.1.1/Rev Test #5.....	170

FIA_X509_EXT.1.1/Rev Test #6.....	170
FIA_X509_EXT.1.1/Rev Test #7.....	171
FIA_X509_EXT.1.2/Rev Test #1.....	172
FIA_X509_EXT.1.2/Rev Test #2.....	173
FIA_X509_EXT.2 Test #1 .....	174
FIA_X509_EXT.3 Test #1 .....	175
FIA_X509_EXT.3 Test #2 .....	176
<b>15.1.6        MACsec.....</b>	<b>176</b>
FAU_GEN.1/MACSEC Test #1 .....	176
FCS_MACSEC_EXT.1 Test #1 .....	177
FCS_MACSEC_EXT.1 Test #2 .....	178
FCS_MACSEC_EXT.2 Test #1 .....	178
FCS_MACSEC_EXT.2 Test #2 .....	179
FCS_MACSEC_EXT.4 Test #1 .....	180
FCS_MACSEC_EXT.4 Test #2 .....	180
FCS_MKA_EXT.1.2 Test #1 .....	181
FCS_MKA_EXT.1.4 Test #1 .....	182
FCS_MKA_EXT.1.4 Test #2 .....	182
FCS_MKA_EXT.1.5 Test #1 .....	183
FCS_MKA_EXT.1.5 Test #2 .....	184
FCS_MKA_EXT.1.8 Test #1 .....	185
FCS_MKA_EXT.1.8 Test #2a .....	186
FCS_MKA_EXT.1.8 Test #2b.....	186
FCS_MKA_EXT.1.8 Test #2c .....	187
FCS_MKA_EXT.1.8 Test #2d.....	188
FCS_MKA_EXT.1.8 Test #2e .....	188
FIA_AFL.1/MACSEC Test #1 .....	189

FIA_AFL.1/MACSEC Test #3 .....	190
FIA_PSK_EXT.1/MACSEC Test #1 .....	190
FIA_PSK_EXT.1/MACSEC Test #2 .....	191
FIA_PSK_EXT.1/MACSEC Test #3 .....	192
FMT_SMF.1/MACSEC Test #1 .....	193
FMT_SMF.1/MACSEC Test #2 .....	194
FMT_SMF.1/MACSEC Test #3a .....	195
FMT_SMF.1/MACSEC Test #3b .....	196
FMT_SMF.1/MACSEC Test #4 .....	197
FPT_FLS.1(2)/SelfTest Test #1 .....	197
FPT_RPL.1 Test #1 .....	199
FPT_RPL.1 Test #2 .....	200
<b>16 Security Assurance Requirements.....</b>	<b>200</b>
<b>16.1.1 ADV_FSP.1 Basic Functional Specification .....</b>	<b>200</b>
ADV_FSP.1 .....	200
ADV_FSP.1 Activity 1 .....	200
<b>16.1.2 AGD_OPE.1 Operational User Guidance .....</b>	<b>201</b>
AGD_OPE.1 .....	201
AGD_OPE.1 Activity 1 .....	201
AGD_OPE.1 Activity 2 .....	201
AGD_OPE.1 Activity 3 .....	202
AGD_OPE.1 Activity 4 .....	202
AGD_OPE.1 Activity 5 [TD0536] .....	202
<b>16.1.3 AGD_PRE.1 Preparative Procedures.....</b>	<b>203</b>
AGD_PRE.1 .....	203
AGD_PRE.1 Activity 1 .....	203
AGD_PRE.1 Activity 2 .....	205
AGD_PRE.1 Activity 3 .....	207



	AGD_PRE.1 Activity 4.....	207
	AGD_PRE.1 Activity 5.....	207
<b>16.1.4</b>	<b>ALC Assurance Activities .....</b>	<b>208</b>
	ALC_CMC.1 .....	208
	ALC_CMC.1 Activity 1.....	208
	ALC_CMS.1.....	208
	ALC_CMS.1 Activity 1.....	208
<b>16.1.5</b>	<b>ATE_IND.1 Independent Testing – Conformance .....</b>	<b>209</b>
	ATE_IND.1.....	209
	ATE_IND.1 Activity 1 .....	209
<b>16.1.6</b>	<b>AVA_VAN.1 Vulnerability Survey .....</b>	<b>209</b>
	AVA_VAN.1 .....	209
	AVA_VAN.1 Activity 1 .....	209
	AVA_VAN.1 Activity 2 .....	211
<b>17</b>	<b>Conclusion.....</b>	<b>212</b>

# 1 TOE Overview

## 1.1 TOE Overview

The Cisco 8000 Series Routers (herein after referred to as the C8000) is a purpose-built, routing platform that also supports MACsec encryption. The TOE includes the hardware models as defined in Table 4 of the ST.

## 1.2 TOE Description

This section provides an overview of the C8000 Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE is comprised of both software and hardware. The hardware is comprised of the following: 8808-SYS, 8812-SYS and 8818-SYS. The software is comprised of the Cisco IOS-XR 7.3.

The TOE consists of a number of components including:

- Chassis: The TOE chassis includes 16 RU (8 slot), 21 RU (12 slot) and 33 RU (18 slot) form factors. The chassis is the component of the TOE in which all other TOE components are housed.
- Route Processor (RP): A route processor in each chassis provide the advanced routing capabilities of the TOE. They also monitor and manage the other components in the C8000.
- Fabric Cards: 8808-FC, 8812-FC and 8818-FC
- Supporting Line Cards: 8800-LC-48H and 8800-LC-36FH

# 2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the NDcPP 2.2e & MACsec EP v1.2 based upon the core SFRs and those implemented based on selections within the PP.

# 3 Test Equivalency Justification

## 3.1 Architectural Description

The Cisco 8000 comprise the TOE. All the possible TOE chassis are listed below:

- 8808-SYS
- 8812-SYS
- 8818-SYS

The hardware is comprised of the following: 8808-SYS, 8812-SYS, 8818-SYS. The software is comprised of the Cisco IOS-XR 7.3


The TOE consists of a number of components including:


- Chassis: The TOE chassis includes 16 RU (8 slot), 21 RU (12 slot) and 33 RU (18 slot) form factors. The chassis is the component of the TOE in which all other TOE components are housed.
- Route Processor (RP): A route processor in each chassis provide the advanced routing capabilities of the TOE. They also monitor and manage the other components in the C8000.
- Data is secured at Layer 2 with MACsec. MACsec-supporting hardware 8800-LC-48H which includes the Cisco IOS-XR software.
- Non MACsec Line Card - 8800-LC-36FH

### 3.2 Specification of Differences

The following tables provide a description of the physical differences between hardware models. None of the listed hardware differences have any impact of the security functionality provided by the TSF. All operate identically.

Table 1 Hardware Models and Specifications

Hardware	Picture	Features
<p>Cisco 8000 Series Routers (C8000)</p> <p>8808-SYS</p> <p>8812-SYS</p> <p>8818-SYS</p> <p>8800-RP</p> <p>8808-FC</p> <p>8812-FC</p> <p>8818-FC</p> <p>8800-LC-48H</p> <p>8800-LC-36FH</p>	 <p style="text-align: center;">8800-LC-48H</p>	<p><b>Physical dimensions (H x W x D)</b></p> <ul style="list-style-type: none"> <li>• 8808: 28 x 17.45 x 33.73 in. (71.12 x 44.32 x 85.7 cm) – 16 RU – 8 line cards</li> <li>• 8812: 36.75 x 17.45 x 35.43 in. (93.345 x 44.23 x 90 cm) – 21 RU – 12 line cards</li> <li>• 8818: 57.75 x 17.45 x 35.43 in. (146.7 x 44.23 x 90 cm) – 33 RU – 18 line cards</li> </ul> <p><b>Route Processors (RP)</b></p> <ul style="list-style-type: none"> <li>• Intel Xeon D-1530 (Broadwell) CPU</li> <li>• 32 GB of DRAM</li> <li>• RS-232 console</li> <li>• 10 GbE SFP+</li> <li>• 1 GbE Management</li> <li>• 2x USB2.0</li> </ul> <p><b>Interfaces</b></p> <ul style="list-style-type: none"> <li>• 48 QSFP28 100 GbE</li> <li>• 36 QSFP56-DD 400 GbE</li> </ul> <p><b>Power</b></p>

Hardware	Picture	Features
	 <p data-bbox="558 552 695 575">8800-LC-36FH</p>	<ul style="list-style-type: none"> <li data-bbox="922 268 1458 323">• 8808 and 8812 – 9 high-voltage power supplies or 12 48V DC power supplies</li> <li data-bbox="922 331 1458 386">• 8818 - 18 high-voltage power supplies or 24 48V DC power supplies</li> </ul>

### 3.3 Equivalency Analysis

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 NDcPP v2.2E & MACSEC EP v1.2.

### 3.4 Platform/Hardware Dependencies

The TOE boundary is inclusive of all hardware required by the TOE. All security functionality is implemented in Platform Independent code which is line-by-line identical across hardware models. The hardware within the TOE only differs by performance.

The hardware is comprised of the following models: 8808-SYS, 8812-SYS and 8818-SYS.

The TOE is a hardware that makes up the router models as follows:

- Chassis: 8808-SYS, 8812-SYS and 8818-SYS
- Route Processors (RP): 8800-RP
- Fabric Cards: 8808-FC, 8812-FC and 8818-FC
- Supporting Line Cards: 8800-LC-48H and 8800-LC-36FH

In case of hardware models 8808-SYS, 8812-SYS and 8818-SYS, the difference is in the physical dimensions of the chassis and the number of Line Cards supported by each chassis. They support 8, 12, and 18 Line Cards respectively. Each model supports the same Route Processor, 8800-RP, uses Intel Xeon D-1530 (Broadwell) central processing unit.

Each model supports the same Line Cards, 8800-LC-48H and 8800-LC-36FH. The 8800-LC-36FH does not support MACsec whereas 8800-LC-48FH support MACsec on all of its 48-ports. The TOE supports MACsec using the CoMIRA Mentor Questa Sim 10.7 processor. The TOE authenticates and encrypts packets between itself and a MACsec peer.

Hence all three models are considered equivalent and full suite of testing needs to be done on any one model with a Route Processor and 8800-LC-48H (MACsec Line Card).

Result: All platforms are equivalent

### 3.5 Software/OS Dependencies:

This category of differences is only applicable if the TOE is installed on an OS outside of the TOE boundary. In this case, all software including the OS is included in IOS-XR and within the TOE boundary. There are no specific dependencies on the OS since the TOE will not be installed on different OSs. The image used on -8808-SYS, 8812-SYS, 8818 is IOS-XR 7.3.

Result: All platforms are equivalent

### 3.6 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 CAVP validated crypto module to provide its cryptographic functionality. This is the same across platforms.

Result: All platforms are equivalent

### 3.7 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 platforms are equivalent

### 3.8 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 IOS-XR software.

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

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

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v2.2e and MACsec EP v1.2 as necessary to satisfy testing/assurance measures prescribed therein.

#### **Security Audit**

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each

auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the administrator with a circular audit trail. The TOE is configured to transmit its audit messages to an external syslog server over an encrypted channel using TLS.

**Cryptographic Support**

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operational Environment – Intel Xeon D-1530 (Broadwell)). In addition, the TOE supports MACsec using the CoMIRA Mentor Questa Sim 10.7 processor (see Table 2 for certificate references).

**Table 2 FIPS References**

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
AES	Used for symmetric encryption/decryption	CBC (128 and 256)	FOM 6.2	A388	FCS_COP.1/DataEncryption FCS_COP.1(1)/KeyedHash:CMAC  FCS_COP.1(2) Cryptographic Operation
		GCM (128 and 256)			
		CTR (128 and 256)			
		AES Key Wrap and CMAC (128 and 256)			
		GCM (128 and 256)	MACsec	C1668	
SHS (SHA-1, SHA-256, SHA-512)	Cryptographic hashing services	Byte Oriented	FOM 6.2	A388	FCS_COP.1/Hash
HMAC (HMAC-SHA-1, SHA-256, SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	FOM 6.2	A388	FCS_COP.1/KeyedHash

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	FOM 6.2	A388	FCS_RBG_EXT.1
RSA	Signature Verification and key transport	PKCS#1 v.1.5, 3072 bit key, FIPS 186-4 Key Gen	FOM 6.2	A388	FCS_CKM.1 FCS_COP.1/SigGen

The TOE provides cryptography in support of remote administrative management via SSHv2 and secures the session between the C8000 and remote syslog server using TLS.

The TOE authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers.

The cryptographic services provided by the TOE are described in Table 3 below:

**Table 3 TOE Provided Cryptography**

Cryptographic Method	Use within the TOE
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in SSH session establishment. Used in TLS session establishment. X.509 certificate signing.
SHS	Used to provide SSH traffic integrity verification Used for keyed-hash message authentication
AES	Used to encrypt SSH session traffic. Used to encrypt TLS session traffic. Used to encrypt MACsec traffic.
RSA	Used to provide cryptographic signature services
HMAC	Used for keyed hash, integrity services in SSH session establishment.
TLS	Used to secure traffic to the syslog server.

## Identification & Authentication

The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules.

After a configurable number of incorrect login attempts, C8000 will lockout the account until a configured amount of time for lockout expires.

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections.

### **Security Management**

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users, all identification and authentication, all audit functionality of the TOE, all TOE cryptographic functionality, the timestamps maintained by the TOE, and updates to the TOE. The TOE supports a privileged administrator role. Only the privileged administrator can perform the above security relevant management functions.

Administrators can create configurable login banners to be displayed at time of login, and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

### **Protection of the TSF**

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally Cisco IOS-XR is not a general-purpose operating system and access to Cisco IOS-XR memory space is restricted to only Cisco IOS-XR functions.

The TOE is also able to detect replay of information received via secure channels (MACsec). The detection applied to network packets that terminate at the TOE, such as trusted communications between the TOE and an IT entity (e.g., MACsec peer). If replay is detected, the packets are discarded.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software



### TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

### Trusted Path/Channels

The TOE establishes a trusted path between the appliance and the CLI using SSHv2 and the syslog server using TLS. MACsec is used to secure communication channels between MACsec peers at Layer 2.

Result: All platforms are equivalent

## 3.9 Difference Comparison

The below table shows the comparison between different chassis and it show that 8818, 8812 & 8808 are equivalent.

- The Cisco 8818 is a 33-RU router that supports distributed forwarding across multiple field replaceable units (FRUs).
- The Cisco 8812 is a 21-RU router that supports distributed forwarding across multiple field replaceable units (FRUs).
- The Cisco 8808 is a 16-RU router that supports distributed forwarding across multiple field replaceable units (FRUs).

### Cisco 8818 Router Components

Component	Quantity
Line cards	18
Route Processors	2
Fabric Cards	8
Fan trays	4
Power trays	6
Power supplies	HVAC/HVDC—18 (3 per tray) DC60—24 (4 per tray) DC100—24 (4 per tray)

### Cisco 8812 Router Components

Component	Quantity
Line cards	12
Route Processors	2
Fabric Cards	8
Fan trays	4
Power trays	3
Power supplies	HVAC/HVDC—9 (3 per tray) DC60—12 (4 per tray) DC100—12 (4 per tray)

### Cisco 8808 Router Components

Component	Quantity
Line cards	8
Route Processors	2
Fabric Cards	8
Fan trays	4
Power trays	3
Power supplies	HVAC/HVDC—9 (3 per tray) DC60—12 (4 per tray) DC100—12 (4 per tray)

As shown above hardware models 8808-SYS, 8812-SYS and 8818-SYS, the difference is in the physical dimensions of the chassis and the number of Line Cards supported by each chassis. They support 8, 12, and 18 Line Cards respectively. Each model supports the same Route Processor, 8800-RP, which uses Intel Xeon D-1530 (Broadwell) central processing unit.

Each model supports the same Line Cards, 8800-LC-48H and 8800-LC-36FH. The 8800-LC-36FH does not support MACsec whereas 8800-LC-48FH support MACsec on all of its 48-ports. The TOE supports MACsec using the CoMIRA Mentor Questa Sim 10.7 processor. The TOE authenticates and encrypts packets between itself and a MACsec peer.

Hence all three models are considered equivalent and full suite of testing needs to be done on any one model with a Route Processor and 8800-LC-48H (MACsec Line Card).

### 3.10 MACsec Analysis

The evaluation team reviewed the ST and examined the TOE hardware models including an ASIC used for MACsec. All TOE models utilize the same ASIC for MACsec functionality. The ASIC used for MACsec has a CAVP certificate for AES.

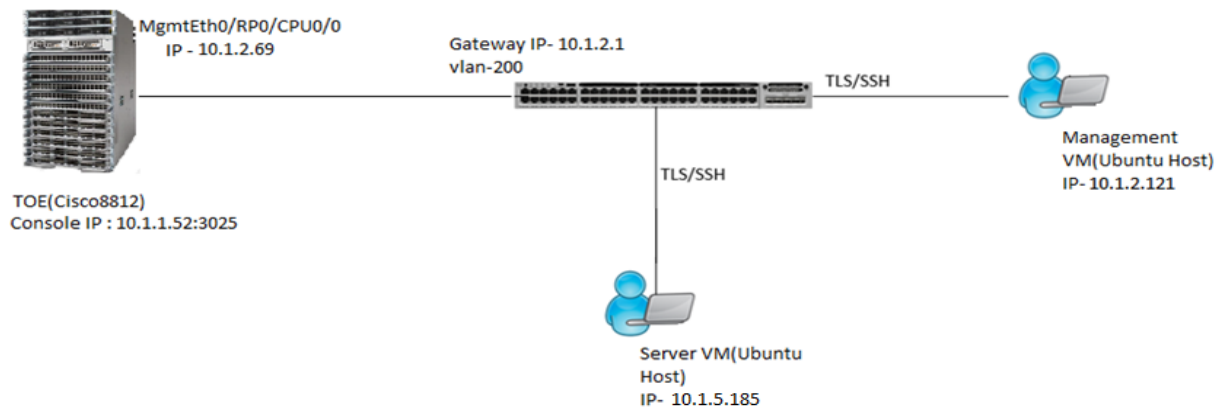
### 3.11 Conclusions

Based on the equivalency rationale listed above, full set of testing was performed on the following subset:

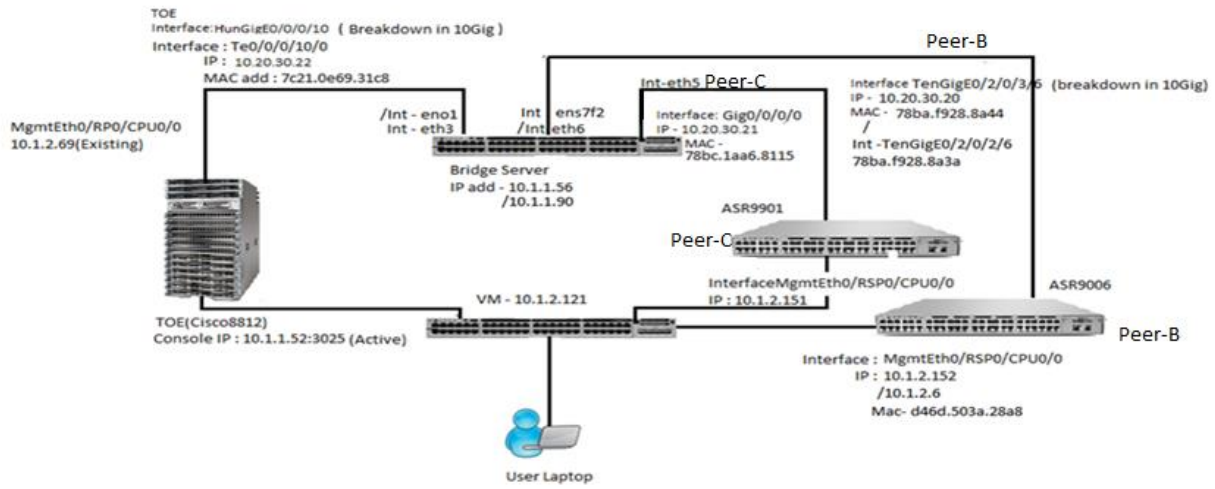
8812-SYS: with RP8800, running Cisco IOS-XR 7.3, with 8812-FC card and 8800-LC-48H MACsec supporting Line card

## 4 Test Bed Descriptions

### 4.1 Test Bed – Audit, Auth, SSHS, TLSC, Update, X509-Rev



### 4.2 Test Bed – MACsec



### 4.3 Labgram

The following table includes all information that is required to be documented for common criteria certification as per NIAP policy.

Name	OS	Function	Protocol	IP address	MAC address	Time	Tools & version
C8812	IOS-XR 7.3	Target of Evaluation	SSH/TLS	10.1.2.69	08ec.f5c2.ec50	Manually set and verified	
			MACsec	10.20.30.20	7c21:0e69:31c8		
ASR9901	IOS-XE 16.12	MACsec peer C	SSH	10.1.2.151	N/A	Manually set and verified	
			MACsec	10.20.30.21	78bc.1aa6.8115		
ASR9006	IOS-XE 16.12	MACsec peer B	SSH	10.1.2.152 / 10.1.2.6	d46d.503a.28a8	Manually set and verified	
			MACsec	10.20.30.22	78ba.f928.8a44 / 78ba.f928.8a3a		
Bridge server	Ubuntu 18.04.4 LTS	MACsec bridge	SSH	10.1.1.56 / 10.1.1.90	e8:ea:6a:27:b6:79	Manually set and verified	Acumen-macsec tool v1.2, Wirehshark2.6.1, acumen-macsec- NEW tool v1.0
Wakko Console	3.16.6u4	Console	SSH	10.1.1.52:3025	N/A	Manually set and verified	
Test user Laptop	Windows 10 pro	Test workstation	SSH/RDP	192.168.254.112	54-14-F3-E8-C4- 2A	Manually set and verified	Putty 0.76, XCA 2.4.0, winSCP 5.19.2
Test VM	Ubuntu 20.04.2 LTS	CRL server	SSH/TLS	10.1.2.121	00:0c:29:ef:72:30	Manually set and veri fied	Wirehshark3.4.6, rsyslogd 8.2001.0, OpenSSL 1.1.1f, acumen-tlsc2.2e & acumen-tlsc, OpenSSH_8.2p1
		Syslog server		10.1.5.185	00:0c:29:ef:72:30		

## Test Time & Location

All testing was carried out at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from September 2021 to September 2022.

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept in a secure repository.

## 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	<p>The evaluator examined the section 6.1 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:</p> <p>Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred such as generating keys, including the type of key and a key reference.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
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 5 titled "Security Relevant Events" in the AGD to verify that it provides an example of each auditable event required by FAU_GEN.1. Each event listed in the NDcPP and MACsec EP is also listed in AGD. Next, the evaluator reexamined AGD and found that the section titled "Security Relevant Events" contains a listing and description of each of the fields in generated audit records that contain the information required in FAU_GEN.1.2.

	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 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.		
Evaluator Findings	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:		
	<b>Administrative Activity</b>	<b>Method (Command Configuration)</b>	<b>Section</b>
	Startup of Audit function	logging trap debugging	3.3.2
	Shutdown of Audit function	no logging trap debugging	3.3.2
	Logout	Exit	3.2.7
	Generating Keys / certificates	crypto key generate rsa	3.3.1 3.3.3
	Configuring Login failure threshold	authen-max-attempts 5	3.2.8
	Display system information	Show version	2
	Configuring CAs	crypto ca trustpoint	3.3.3

Generating CSRs	crypto ca enroll <name>	3.3.3
Performing Software Updates	A series of CLI commands are provided for performing updates	4.5
Setting the Time	clock set	4.3
Configuring Admin Timeout	exec-timeout <time>	3.2.6
Configuring the Audit Server	logging host	3.3.2
Configuring Access Banner	Banner login	4.4
Setting Password Length	aaa password-policy policy	4.2
Configuring SSH	ssh server configurations	3.2.5 3.3.1
MACsec Configuration	A series of CLI commands are provided for configuration of MACsec	3.3.5

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.

Administrative Activity	Test Case(s)
Startup	FMT_MOF.1/Services Test #1
Shutdown	FMT_MOF.1/Services Test #1
Login	FTA_SSL.4 Test #2
Logout	FTA_SSL.4 Test #2
Generating Keys (certificates)	FCS_IPSEC_EXT.1.13 T1 FMT_MOF.1/Services Test #1



	Deleting Keys (certificates)	FMT_MTD.1/CryptoKeys Test #2
	Resetting Passwords	FMT_SMF.1
	Configuring CAs	FIA_X509_EXT.1.1/Rev T1
	Generating CSRs	FIA_X509_EXT.3 T1
	Performing Software Updates	FPT_TUD_EXT.1 T1
	Setting the Time	FPT_STM_EXT.1 T1
	Configuring Admin Timeout	FTA_SSL_EXT.1 T1
	Configuring the Audit Server	FAU_GEN.1 T1
	Configuring Access Banner	FTA_TAB.1 T1
	Setting Password Length	FIA_PMG_EXT.1 T1
	Configuring SSH	FCS_SSHS_EXT.1.4 T1
	MACsec Configuration	FCS_MACSEC_EXT.1 T1
<p>The above analysis illustrates that each of the relevant configuration methods is appropriately audited by the TOE.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>		
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 section 6.1 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 TOE is a standalone TOE configured to export syslog records to a specified, external syslog server in real-time.

	<p>The TOE protects communications with an external syslog server via TLS. If the connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents when connected to the syslog server.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 5.1.2.2 FAU\_STG\_EXT.1 TSS 2

Objective	<p>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.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 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 For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 2097152 to 125000000 bytes of available disk space.</p> <p>Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 5.1.2.3 FAU\_STG\_EXT.1 TSS 3

Objective	<p>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.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> 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</p>

	<p>The TOE is a standalone TOE configured to export syslog records to a specified, external syslog server in real-time.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 5.1.2.4 FAU\_STG\_EXT.1 TSS 4

Objective	<p>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.</p>
Evaluator Findings	<p>The evaluator examined the 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:</p> <p>For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 2097152 to 125000000 bytes of available disk space.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 5.1.2.5 FAU\_STG\_EXT.1 TSS 5

Objective	<p>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.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 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 TOE is configured to export syslog records to a specified, external syslog server in real-time. The TOE protects communications with an external syslog server via TLS. If the connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents when connected to the syslog server.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
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	<p>The evaluator examined the section 3.3.2 titled “Logging Configuration” and section 3.3.4 titled “Logging to syslog server via TLS” 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 states that:</p> <p>Logging of all required audit events related to TOE security functions must be enabled.</p> <p>Note: To get some of the required audit records with the required information, debugging may need to be turned on/configured. In doing so, a large amount of audit records may be generated.</p> <ol style="list-style-type: none"> <li>1. RP/0/RSP0/CPU0: router# <b>configure</b></li> <li>2. RP/0/RSP0/CPU0: router (config)#<b>logging trap debugging</b></li> <li>3. RP/0/RSP0/CPU0: router (config)#<b>logging 10.34.0.1 vrf default severity debugging</b></li> <li>4. RP/0/RSP0/CPU0: router (config)#<b>logging hostnameprefix TOE: C8000</b></li> <li>5. RP/0/RSP0/CPU0: router (config)#<b>service timestamps log datetime year localtime msec</b></li> <li>6. RP/0/RSP0/CPU0: router (config)#<b>service timestamps debug datetime year localtime msec</b></li> <li>7. RP/0/RSP0/CPU0: router (config)# <b>aaa accounting commands default start-stop local</b></li> <li>8. RP/0/RSP0/CPU0: router (config)#<b>commit</b></li> <li>9. RP/0/RSP0/CPU0: router (config)#<b>end</b></li> </ol> <p>This example shows how to set the maximum log file size to 10 MB:</p> <pre>RP/0/RSP0/CPU0: router(config)# logging buffered &lt;2097152-125000000&gt;</pre> <p>The following example shows how to enable configuration logging:</p> <pre>RP/0/RSP0/CPU0: router# <b>configure</b> RP/0/RSP0/CPU0: router (config)# <b>logging trap debugging</b></pre> <p>Using a secure TLS connection for Syslog Server is required in the evaluated configuration: The minimum TLS version for use to TLSv1.1 and TLSv1.2 with support for the following ciphers that are available by default in FIPS mode.</p>

	<ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> </ul> <p>logging to the syslog server via TLS needs to be setup. . To protect against audit data loss the TOE must be configured to send the audit records securely (via TLS) to an external Secure Syslog Server. You can use the server hostname for this configuration. Based on the configured severity, the router sends syslogs to the server. Logging severity options include alerts, critical, debugging, emergencies, errors, informational, notifications and warnings.</p> <pre>RP/0/RP0/CPU0: router #conf RP/0/RP0/CPU0: router (config)#logging tls-server syslog server name RP/0/RP0/CPU0: router (config-logging-tls-peer)# severity debugging RP/0/RP0/CPU0: router (config-logging-tls-peer)# address ipv4 ip address RP/0/RP0/CPU0: router (config-logging-tls-peer)# commit</pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
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	<p>The evaluator examined the section 5 titled “Security Relevant Events” 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:</p> <p>The TOE is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as simultaneously offloaded to an external syslog server.</p> <p>... When configured for a syslog backup the TOE will simultaneously offload events from a separate buffer to the external syslog server. This buffer is used to queue events to be sent to the syslog server if the connection to the server is lost. It is a circular buffer, so when the events overrun the storage space overwrites older events.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
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.
-----------	--

<p>Evaluator Findings</p>	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> in the ST 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 ST states that:</p> <p>For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 2097152 to 125000000 bytes of available disk space.</p> <p>The evaluator examined the section 5 titled “Security Relevant Events” in the AGD to verify that it corresponds with the ST selection for FAU_STG_EXT.1.3. Upon investigation, the evaluator found that the AGD states that:</p> <p>The local log buffer is circular. Newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer.</p> <p>When configured for a syslog backup the TOE will simultaneously offload events from a separate buffer to the external syslog server. This buffer is used to queue events to be sent to the syslog server if the connection to the server is lost. It is a circular buffer, so when the events overrun the storage space overwrites older events.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass.</p>

## 6 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.

### 6.1.1 FCS\_CKM.1

#### FCS\_CKM.1 TSS 1

<p>Objective</p>	<p>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.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section 6.1 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:</p> <p>The TOE implements DH group 14 key establishment schemes that meets RFC 3526, Section 3. The TOE acts as both a sender and receiver for Diffie-Helman based key establishment schemes.</p>

	<p>The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP 800-56A and with section 6.</p> <p>The TOE can create an RSA public-private key pair, with a minimum RSA key size of 2048-bit.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 3.2.5 titled “Enabling FIPS mode” 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:</p> <ul style="list-style-type: none"> <li>• Generate the crypto key for SSH using the “<b>crypto key generate rsa</b>” command.</li> <li>• Generate RSA key material – choose a longer modulus length for more secure keys (i.e. 2048 for RSA):  RP/0/RSP0/CPU0:router# <b>crypto key generate rsa general-keys rsakeypair</b>   RP/0/RSP0/CPU0:router# How many bits in the modulus [512]: <b>2048</b>   RP/0/RSP0/CPU0:router#<b>show crypto key mypubkey rsa</b></li> </ul> <p>RSA keys are generated in pairs—one public RSA key and one private RSA key. This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.</p> <p>No specific TOE configuration is required for the use of RSA in TLS protocol. The Section 3.3.2.4 of the AGD states:</p> <p>Using a secure TLS connection for Syslog Server is required in the evaluated configuration: TLS 1.2 with support for the following ciphers that are available by default in FIPS mode.</p> <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> </ul> <p>Regarding the use of ‘safe primes’, AGD section 3.3.1 states that:</p> <p>Telnet for management purposes is disabled by default. IOS XR only supports SSHv2 with the following by default.</p> <ul style="list-style-type: none"> <li>• encryption algorithms, aes128-ctr, aes256-ctr, hmac-sha2-256 and hmac-sha2-512 to ensure confidentiality of the session.</li> <li>• hashing algorithms hmac-sha1to ensure the integrity of the session.</li> </ul>

	<ul style="list-style-type: none"> <li>SSH transport implementation public key algorithms: ssh-rsa.</li> <li>Key Exchange Algorithms: diffie-hellman-group14-sha1</li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 6.1.2 FCS\_CKM.2

#### 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	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> 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:</p> <p>The TOE implements DH group 14 key establishment schemes that meets RFC 3526, Section 3. The TOE acts as both a sender and receiver for Diffie-Helman based key establishment schemes.</p> <p>The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP 800-56A and with section 6.</p> <p>The TOE can create an RSA public-private key pair, with a minimum RSA key size of 2048-bit.</p> <p>RSA scheme can be used to generate a Certificate Signing Request (CSR). Via offline CSR or Simple Certificate Enrollment Protocol (SCEP), the TOE can: send the CSR to a Certificate Authority (CA) for the CA to generate a certificate; and receive its X.509 certificate from the CA. Integrity of the CSR and certificate during transit are assured through use of digital signatures (encrypting the hash of the TOE's public key contained in the CSR and certificate). The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). The IOS-XR Software supports embedded PKI client functions that provide secure mechanisms for distributing, managing, and revoking certificates. The TOE can also use X.509v3 certificates for authentication of TLS sessions.</p> <p>The TOE acts as both a sender and receiver for RSA -based key establishment schemes. The RSA key establishment meets the RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.</p> <table border="1" data-bbox="495 1705 1318 1860"> <thead> <tr> <th>Scheme</th> <th>SFR</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>RSA Key generation</td> <td>FCS_SSHS_EXT.1</td> <td>SSH Remote Administration</td> </tr> </tbody> </table>	Scheme	SFR	Service	RSA Key generation	FCS_SSHS_EXT.1	SSH Remote Administration
Scheme	SFR	Service					
RSA Key generation	FCS_SSHS_EXT.1	SSH Remote Administration					



		Key establishment	FCS_TLSC_EXT.1	Support for SSH and TLS key establishment
		FFC Key generation Key establishment	FCS_SSHS_EXT.1	SSH Remote Administration
			FIA_X509_EXT.1/Rev FIA_X509_EXT.2 FIA_X509_EXT.3	Transmit generated audit data to an external IT entity
	Based on these findings, this assurance activity is considered satisfied.			
Verdict	Pass.			

### 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	<p>The evaluator examined the section 3.2.5 titled “Enabling FIPS mode” &amp; section 3.3.1 “SSH public-key based authentication” 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 states that:</p> <ul style="list-style-type: none"> <li>• Generate the crypto key for SSH using the “<b>crypto key generate rsa</b>” command.</li> <li>• Generate RSA key material – choose a longer modulus length for more secure keys (i.e. 2048 for RSA):  RP/0/RSP0/CPU0:router# <b>crypto key generate rsa general-keys rsakeypair</b>   RP/0/RSP0/CPU0:router# How many bits in the modulus [512]: <b>2048</b>   RP/0/RSP0/CPU0:router#<b>show crypto key mypubkey rsa</b></li> </ul> <p>RSA keys are generated in pairs—one public RSA key and one private RSA key. This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.</p> <p>No specific TOE configuration is required for the use of RSA in TLS protocol. The Section 3.3.2.4 of the AGD states:</p> <p>Using a secure TLS connection for Syslog Server is required in the evaluated configuration: TLS 1.2 with support for the following ciphers that are available by default in FIPS mode.</p> <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> </ul>

	<p>To configure key-exchange algorithms</p> <pre>RP/0/RP0/CPU0: router(config)#ssh server algorithms key-exchange diffie-hellman-group14-sha1</pre> <pre>RP/0/RP0/CPU0: router(config)#commit</pre> <pre>RP/0/RSP0/CPU0: router #crypto key gen rsa</pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 6.1.3 FCS\_CKM.4

#### FCS\_CKM.4 TSS 1

Objective	<p>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 for<sup>2</sup>). 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.</p>											
Evaluator Findings	<p>The evaluator examined the section 6.1 and section 7 titled <b>TOE Summary Specification</b> and <b>Key Zeroization</b>, respectively 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 secure channel protocol), and the destruction method used in each case. Upon investigation, the evaluator found that the TSS states that:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Description of Key</th> <th>Zeroization</th> </tr> </thead> <tbody> <tr> <td>Diffie-Hellman Shared Secret</td> <td>This is the shared secret used as part of the Diffie-Hellman key exchange. This key is stored in DRAM.</td> <td>Automatically after completion of DH exchange.  Overwritten with: 0x00</td> </tr> <tr> <td>Diffie Hellman private exponent</td> <td>This is the private exponent used as part of the Diffie-Hellman key exchange. This key is stored in DRAM.</td> <td>Zeroized upon completion of DH exchange.  Overwritten with: 0x00</td> </tr> </tbody> </table>			Name	Description of Key	Zeroization	Diffie-Hellman Shared Secret	This is the shared secret used as part of the Diffie-Hellman key exchange. This key is stored in DRAM.	Automatically after completion of DH exchange.  Overwritten with: 0x00	Diffie Hellman private exponent	This is the private exponent used as part of the Diffie-Hellman key exchange. This key is stored in DRAM.	Zeroized upon completion of DH exchange.  Overwritten with: 0x00
Name	Description of Key	Zeroization										
Diffie-Hellman Shared Secret	This is the shared secret used as part of the Diffie-Hellman key exchange. This key is stored in DRAM.	Automatically after completion of DH exchange.  Overwritten with: 0x00										
Diffie Hellman private exponent	This is the private exponent used as part of the Diffie-Hellman key exchange. This key is stored in DRAM.	Zeroized upon completion of DH exchange.  Overwritten with: 0x00										

MACsec Security Association Key (SAK)	The SAK is used to secure the control plane traffic. This key is stored in internal ASIC register.	Automatically when MACsec session terminated.  Overwritten with: 0x00
MACsec Connectivity Association Key (CAK)	The CAK secures the control plane traffic. This key is stored in internal ASIC register.	Automatically when MACsec session terminated.  Overwritten with: 0x00
MACsec Key Encryption Key (KEK)	The Key Encrypting Key (KEK) is used by Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a Secure Connectivity Association (CA). This key is stored in internal ASIC register.	Automatically when MACsec session terminated.  Overwritten with: 0x00
MACsec Integrity Check Key (ICK)	The ICK is used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, This key is stored in internal ASIC register.	Automatically when MACsec session terminated.  Overwritten with: 0x00
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents) using memset. This overwrites the key with all 0's. This key is stored in NVRAM.	Zeroized using the following command:  <b># crypto key zeroize rsa</b>  Overwritten with: 0x00
SSH Session Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no	Automatically when the SSH session is terminated.

		matter its contents). This is called by the ssh_close function when a session is ended. This key is stored in DRAM.	Overwritten with: 0x00
	User Password	This is a variable 15+ character password that is used to authenticate local users. The password is stored in NVRAM.	Zeroized by overwriting with new password
	Enable Password (if used)	This is a variable 15+ character password that is used to authenticate local users at a higher privilege level. The password is stored in NVRAM.	Zeroized by overwriting with new password
	RNG Seed	This seed is for the RNG. The seed is stored in DRAM.	Zeroized upon power cycle the device
	RNG Seed Key	This is the seed key for the RNG. The seed key is stored in DRAM.	Zeroized upon power cycle the device
	AES Key	The results are zeroized by overwriting the values with 0x00. This is called by the ssh_close function when a session is ended.  This key is stored in DRAM	Automatically when the SSH/TLS session is terminated.  Overwritten with: 0x00
	TLS server private key	This key is used for authentication, so the server can prove who it is. The private key used for SSLv3.1/TLS secure connections. The key is stored in NVRAM.	Zeroized by overwriting with new key
	TLS server public key	This key is used to encrypt the data that is used to compute the secret key. The public key used for SSLv3.1/TLS secure	Zeroized by overwriting with new key

		connection. The key is stored in NVRAM.	
	TLS pre-master secret	The pre-master secret is the client and server exchange of random numbers and a special number, the pre-master secret, This pre-master secret is using asymmetric cryptography from which new TLS session keys can be created. The key is stored in SDRAM.	Automatically after TLS session terminated.  The value is overwritten with "0x00."
	TLS session encryption key	The session encryption key is unique for each session and is based on the shared secrets that were negotiated at the start of the session. The Key is used to encrypt TLS session data. The key is stored in SDRAM.	Automatically after TLS session terminated.  The value is overwritten with "0x00."
	TLS session integrity key	This key is used to provide the privacy and TLS data integrity protection. The key is stored in SDRAM.	Automatically after TLS session terminated. The entire object is overwritten with zeros
	<p>The evaluator found that the description 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>		
Verdict	Pass.		

#### FCS\_CKM.4 TSS 2

Objective	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).
Evaluator Findings	The evaluator examined the <b>FCS_CKM.4</b> entry in section 6.1 titled <b>TOE Summary Specification</b> and the section titled <b>Key Zeroization</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 table provided information on keys stored in non-volatile memory including a description of the interfaces used to destroy keys:

	Name	Description of Key	Zeroization
	SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents) using memset. This overwrites the key with all 0's. This key is stored in NVRAM.	Zeroized using the following command:  <b># crypto key zeroize rsa</b>  Overwritten with: 0x00
	TLS server private key	This key is used for authentication, so the server can prove who it is. The private key used for SSLv3.1/TLS secure connections. The key is stored in NVRAM.	Zeroized by overwriting with new key
	TLS server public key	This key is used to encrypt the data that is used to compute the secret key. The public key used for SSLv3.1/TLS secure connection. The key is stored in NVRAM.	Zeroized by overwriting with new key
	Based on these findings, this assurance activity is considered satisfied.		
Verdict	Pass.		

#### 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 6.1 titled <b>TOE Summary Specification &amp; Key Zeroization</b> 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 no keys are stored in non-plaintext form. All keys are stored in plaintext form and were documented along with their method of zeroization.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

#### 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	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> &amp; titled <b>Key Zeroization</b> 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:</p> <p>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.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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	<p>The TSS entry for FCS_CKM.4 in section 6.1 titled <b>TOE Summary Specification &amp; Key Zeroization</b> of the ST was used to determine the verdict of this assurance activity in addition to Annex A, ‘Key Zeroization’. Upon investigation, the evaluator found that keys are only overwritten with “0x00”</p> <p>The evaluator verified that ST does not specify the use of ‘a value that does not contain any CSP’ to overwrite keys.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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	<p>The evaluator examined 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 that the AGD does not identify any configurations or circumstances that may not strictly conform to the key destruction requirement. This was consistent with the TSS description.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

## 6.1.4 FCS\_COP.1/DataEncryption

### 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	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> 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:</p> <p>The TOE provides symmetric encryption and decryption capabilities using AES in GCM, CTR and CBC mode (128 and 256 bits) as described in ISO 19772 and ISO 10116 respectively. Please see CAVP certificate in Table 5 for validation details. AES is implemented in the SSH protocol. The TOE provides AES encryption and decryption in support of SSHv2 for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 3.3 titled Network Protocols and Cryptographic Settings 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 that:</p> <p>Telnet for management purposes is disabled by default. IOS XR only supports SSHv2 with the following by default.</p> <ul style="list-style-type: none"> <li>• encryption algorithms, aes128-ctr, aes256-ctr to ensure confidentiality of the session.</li> <li>• hashing algorithms hmac-sha1to ensure the integrity of the session.</li> <li>• SSH transport implementation public key algorithms: ssh-rsa.</li> <li>• Key Exchange Algorithms: diffie-hellman-group14-sha1</li> </ul> <p>Using a secure TLS connection for Syslog Server is required in the evaluated configuration: The minimum TLS version for use to TLSv1.1 and TLSv1.2 with support for the following ciphers that are available by default in FIPS mode.</p> <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> </ul>



	Therefore, once the TOE's initial setup is complete, the Security Target selected modes and key sizes are configured by default and they cannot be changed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

#### 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: # A388, #C1668 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

#### 6.1.5 FCS\_COP.1/SigGen

##### 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 section 6.1 titled <b>TOE Summary Specification</b> 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 TOE provides cryptographic signature services using the following: RSA Digital Signature Algorithm with key size of 3072 as specified in FIPS PUB 186-4, "Digital Signature Standard".  The TOE provides cryptographic signatures in support of SSH and TLS for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands. The TOE provides the RSA option in support of SSH key establishment. RSA (3072-bits) is used in the establishment of SSHv2 and TLS key establishment. For SSH, RSA host keys are supported  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

##### 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 section 3.2.5 titled "Enabling FIPS mode" 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 has detailed steps for configuring RSA key and key size.  Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass.
---------	-------

#### 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 RSA SigGen & SigVer (186-4) Certs: # A388 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

#### 6.1.6 FCS\_COP.1/Hash

##### 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 section 6.1 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 TOE provides cryptographic hashing services using SHA-1, SHA-256, and SHA-512 as specified in ISO/IEC 10118-3:2004.  The TOE provides Secure Hash Standard (SHS) hashing in support of SSH and TLS for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

##### 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 verified the AGD section titled Network Protocols and Cryptographic Settings to confirm that No additional configurations are required to configure required hash functions.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

##### FCS\_COP.1/Hash Test/CAVP 1

Objective	The evaluator shall verify the implementation of hashing supported by the TOE.
Evaluator Findings	CAVP SHS Certs: # <b>A388</b> Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

### 6.1.7 FCS\_COP.1/KeyedHash

#### FCS\_COP.1/KeyedHash TSS 1

Objective	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.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled TOE Summary Specification 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:</p> <p>The TOE provides keyed-hashing message authentication services using HMAC-SHA1, HMAC-SHA-256, and HMAC-SHA-512 with key sizes 160, 256, and 512 bits, and message digest size 160, 256, and 512 bits as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.</p> <p>SHA-1, SHA-256, and SHA-512 are the hash function used. The “message digest size” specifies the block size and output MAC length used, which is 160, 256, and 512.</p> <p>Additionally The TOE provides SHS hashing and HMAC message authentication in support of SSHv2, TLSv1.2 for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands. SHS hashing and HMAC message authentication (SHA-1) is used in the establishment of TLS and SSHv2 sessions.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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	<p>The evaluator examined the section 6.1 titled TOE SUMMARY SPECIFICATION in the Security Target and Section 3.3 of the AGD to verify the HMAC function values claimed in the Security Target and 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:</p> <p>Telnet for management purposes is disabled by default. IOS XR only supports SSHv2 with the following by default.</p> <ul style="list-style-type: none"> <li>• encryption algorithms, aes128-ctr, aes256-ctr, hmac-sha2-256 and hmac-sha2-512 to ensure confidentiality of the session.</li> <li>• hashing algorithms hmac-sha1to ensure the integrity of the session.</li> <li>• SSH transport implementation public key algorithms: ssh-rsa.</li> <li>• Key Exchange Algorithms: diffie-hellman-group14-sha1</li> </ul>

	<p>Using a secure TLS connection for Syslog Server is required in the evaluated configuration: The minimum TLS version for use to TLSv1.1 and TLSv1.2 with support for the following ciphers that are available by default in FIPS mode.</p> <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> </ul> <p>Therefore, once the TOE's initial setup is complete, the Security Target selected HMAC functions are configured by default and they cannot be changed.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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: # <b>A388</b> , #C1668 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

### 6.1.8 FCS\_COP.1(1)/KeyedHashCMAC

#### FCS\_COP.1(1)/KeyedHashCMAC TSS 1 [TD0466]

Objective	The evaluator shall examine the TSS to ensure that it specifies the following values used by the AES-CMAC function: key length, hash function used, block size, and output MAC length used.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled "TOE Security Functional Requirement Measures" in the Security Target to verify that the TSS specifies the following values used by the AES-CMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE provides keyed-hash message authentication in accordance with AES-CMAC and cryptographic key sizes 128 and 256 bits with message digest size of 128 bits, block size of 128 bits, and MAC length of 128 bits which meets NIST SP 800-38B.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 6.1.9 FCS\_COP.1(5)

#### FCS\_COP.1(5) TSS 1 [TD0466]

Objective	The evaluator shall verify that the TSS describes the supported AES modes that are required for this EP in addition to the ones already required by the NDcPP.
-----------	--

Evaluator Findings	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the supported AES modes that are required for this EP in addition to the ones already required by the NDcPP. Upon investigation, the evaluator found that the TSS states that: The TOE provides symmetric encryption and decryption capabilities using AES in AES Key Wrap and GCM mode (128 and 256 bits) as described in AES as specified in ISO 18033-3, AES Key Wrap in CMAC mode as specified in NIST SP 800-38F, GCM as specified in ISO 19772. AES is implemented in MACsec protocol.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 6.1.10FCS\_RBG\_EXT.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	<p>The evaluator examined the section 6.1 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:</p> <p>The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in ISO/IEC 18031:2011 seeded by an entropy source that accumulates entropy from a TSF-hardware based noise source.</p> <p>The deterministic RBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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	<p>No configuration is required for implementation of the RNG functionality.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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: #A388 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

## 7 TSS and Guidance Activities (MACsec)

### 7.1.1 FCS\_MACSEC\_EXT.1

#### FCS\_MACSEC\_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the ability of the TSF to implement MACsec in accordance with IEEE 802.1AE-2006.
Evaluator Findings	The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the ability of the TSF to implement MACsec in accordance with IEEE 802.1AE-2006. Upon investigation, the evaluator found that the TSS states that:  The TOE implements MACsec in compliance with IEEE Standard 802.1AE-2006. The MACsec connections maintain confidentiality of transmitted data and takes measures against frames transmitted or modified by unauthorized devices. In addition, the TOE implementation provides configuration options and management of the MACsec functionality.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### FCS\_MACSEC\_EXT.1 TSS 2

Objective	The evaluator shall also determine that the TSS describes the ability of the TSF to derive SCI values from peer MAC address and port data and to reject traffic that does not have a valid SCI.
Evaluator Findings	The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the ability of the TSF to derive SCI values from peer MAC address and port data and to reject traffic that does not have a valid SCI. Upon investigation, the evaluator found that the TSS states that: The SCI is composed of a globally unique 48-bit MAC Address and the Secure System Address (port). The SCI is part of the SecTAG if the SC bit is set and will be at the end of the tag. Any MPDUs during a given session that contain an SCI other than the one used to establish that session is rejected.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

### FCS\_MACSEC\_EXT.1 TSS 3 [TD0553]

Objective	The evaluator shall check the TSS for an assertion that only EAPOL, MACsec Ethernet frames, and MAC control frames are accepted by the MACsec interface.
Evaluator Findings	<p>The evaluator examined the FCS_MACSEC_EXT.1 entry in section titled TOE Summary Specification in the Security Target to verify that the TSS asserts that only EAPOL, MACsec Ethernet frames and MAC control frames are accepted by the MACsec interface. Upon investigation, the evaluator found that the TSS states that:</p> <p>Only EAPOL (PAE EtherType 88-8E), MACsec frames (EtherType 88-E5), and MAC Control frames (EtherType 88-08) are permitted and others are rejected.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

### 7.1.2 FCS\_MACSEC\_EXT.2

#### FCS\_MACSEC\_EXT.2 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the methods that the TOE implements to provide assurance of MACsec integrity, including the confidentiality offset(s) used, the use of an ICV (including the supported length), and generating the ICV with the SAK, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the methods that the TOE implements to provide assurance of MACsec integrity, including the confidentiality offset(s) used, the use of an ICV (including the supported length), and generating the ICV with the SAK, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV. Upon investigation, the evaluator found that the TSS states that: The TOE implements the MACsec requirement for integrity protection with the confidentiality offsets of 0, 30 and 50 through the CLI command of “mka-policy confidentiality-offset command”.</p> <p>An offset value of 0 does not offset the encryption and offset values of 30 and 50 offset the encryption by 30 and 50 characters respectively.</p> <p>An Integrity Check Value (ICV) that is 16 bytes in length is derived with the Secure Association Key (SAK) and is used to provide assurance of the integrity of MPDUs.</p> <p>The TOE derives the ICV from a CAK using KDF, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

## FCS\_MACSEC\_EXT.2 Guidance 1

Objective	If any integrity verifications are configurable such as the confidentiality offset(s) used or the mechanism used to derive an ICK, the evaluator shall verify that instructions for performing these functions are documented.
Evaluator Findings	<p>The evaluator verified that instructions for configuring integrity verification is documented in the TOE guidance documentation. The section titled ‘Configuring MACsec’ of the AGD was used to determine the verdict of this assurance activity. This section provides an external document reference [5] which directs the reader to the <a href="#">System Security Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.3.x</a>. Under Configure MACsec, section titled “Creating a User-Defined MACsec Policy”, appropriate guidance has provided.</p> <ul style="list-style-type: none"> <li>• Configuration of the confidentiality offset, using the conf-offset command.</li> </ul> <p>Based on these findings, this assurance activity is considered satisfied</p>
Verdict	Pass

### 7.1.3 FCS\_MACSEC\_EXT.3

#### FCS\_MACSEC\_EXT.3 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the method used to generate SAKs and nonces and that the strength of the CAK and the size of the CAK’s key space are provided.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the method used to generate SAKs and nonces and that the strength of the CAK and the size of the CAK’s key space are provided. Upon investigation, the evaluator found that the TSS states that:</p> <p>Each SAK is generated using the KDF specified in SP800-108 (KDF Validation System), clause 6.2.1 using the following transform - <math>KS\text{-nonce} = \text{a nonce of the same size as the required SAK, obtained from an RNG each time an SAK is generated.}</math></p> <p>The CAK is based on AES cipher in CMAC mode, with key sizes of 128 and 256 bits. Each of the keys used by MKA is derived from the CAK.</p> <p>The key string is the CAK that is used for ICV validation by the MKA protocol. The CAK is not used directly, but derives two further keys from the CAK using the AES cipher in CMAC mode.</p> <p>The derived keys, which are derived via key derivation function as defined in SP800-108 KDF (CMAC) are tied to the identity of the CAK, and thus restricted to use with that particular CAK. These are the ICV Key (ICK) used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, and the Key Encrypting Key (KEK) used by the Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a CA.</p>



	<p>The size of the key is based on the configured AES key sized used. If using AES 128-bit CMAC mode encryption, the key string will be 32-bit hexadecimal in length. If using 256-bit encryption, the key string will be 64-bit hexadecimal in length.</p> <p>The TOE’s random bit generator is used for creating these unique nonces.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 7.1.4 FCS\_MACSEC\_EXT.4

##### FCS\_MACSEC\_EXT.4 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the SAK is wrapped prior to being distributed using the AES implementation specified in this EP.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes how the SAK is wrapped prior to being distributed using the AES implementation specified. Upon investigation, the evaluator found that the TSS states that: The SAKs are distributed between these peers using AES Key Wrap. Prior to distribution of the SAKs between these peers, the TOE uses AES Key Wrap GCM with a key size of 128 or 256 bits in accordance with AES as specified in ISO 18033-3, AES Key Wrap in CMAC mode as specified in NIST SP 800-38F, and GCM as specified in ISO 19772.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

##### FCS\_MACSEC\_EXT.4 Guidance 1

Objective	The evaluator shall verify that the guidance provides instructions on how to configure peer authentications. The evaluator shall also verify that the method of specifying a lifetime for CAKs is described.
Evaluator Findings	<p>The evaluator verified that instructions for configuring integrity verification is documented in the TOE guidance documentation. The section titled ‘Configuring MACsec’ of the AGD was used to determine the verdict of this assurance activity. This section provides an external document reference [5] which directs the reader to the <a href="#">System Security Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.3.x</a>. Under “Configure MACsec” &amp; “Configuring and Verifying MACSec Encryption”, proper guidance has provided to configure peer authentication, and lifetime for CAK respectively.</p> <p>Based on these findings, this assurance activity is considered satisfied</p>

Verdict	Pass
---------	------

### 7.1.5 FCS\_MKA\_EXT.1

#### FCS\_MKA\_EXT.1.4 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the methods that the TOE implements to provide assurance of MKA integrity, including the use of an ICV and the ability to use a KDF to derive an ICK.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the methods that the TOE implements to provide assurance of MKA integrity, including the use of an ICV and the ability to use a KDF to derive an ICK. Upon investigation, the evaluator found that the TSS states that: For the Data Integrity Check, MACsec uses MKA to generate an Integrity Check Value (ICV) for the frame arriving on the port. If the generated ICV is the same as the ICV in the frame, then the frame is accepted; otherwise it is dropped. The key string is the Connectivity Association Key (CAK) that is used for ICV validation by the MKA protocol.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### FCS\_MKA\_EXT.1.8 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE’s compliance with IEEE 802.1X-2010 and 802.1Xbx-2014 for MKA, including the values for MKA and Hello timeout limits and support for data delay protection.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the TOE’s compliance with IEEE 802.1X-2010 and 802.1Xbx-2014 for MKA, including the values for MKA and Hello timeout limits and support for data delay protection. Upon investigation, the evaluator found that the TSS states that: The TOE implements Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014.</p> <p>The data delay protection is enabled for MKA as a protection guard against an attack on the configuration protocols that MACsec is designed to protect by alternately delaying and delivering their PDUs. The Delay protection does not operate if and when MKA operation is suspended. An MKA Lifetime Timeout limit of 6.0 seconds and Hello Timeout limit of 2.0 seconds is enforced by the TOE.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

### FCS\_MKA\_EXT.1.8 TSS 2

Objective	The evaluator shall also verify that the TSS describes the ability of the PAE of the TOE to establish unique CAs with individual peers and group CAs using a group CAK such that a new group SAK is distributed every time the group’s membership changes.
Evaluator Findings	The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the ability of the PAE of the TOE to establish unique CAs with individual peers and group CAs using a group CAK such that a new group SAK is distributed every time the group’s membership changes. Upon investigation, the evaluator found that the TSS states that: On successful peer authentication, a connectivity association is formed between the peers and a secure Connectivity Association Key Name (CKN) is exchanged. After the exchange, the MKA ICV is validated with a Connectivity Association Key (CAK), which is effectively a secret key.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

### FCS\_MKA\_EXT.1.8 TSS 3

Objective	The evaluator shall also verify that the TSS describes the invalid MKPDUs that are discarded automatically by the TSF in a manner that is consistent with the SFR, and that valid MKPDUs are decoded in a manner consistent with IEEE 802.1X-2010 section 11.11.4.
Evaluator Findings	The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the invalid MKPDUs that are discarded automatically by the TSF in a manner that is consistent with the SFR, and that valid MKPDUs are decoded in a manner consistent with IEEE 802.1X-2010 section 11.11.4. Upon investigation, the evaluator found that the TSS states that: The TOE discards MKPDUs that do not satisfy the requirements listed under FCS_MKA_EXT.1.8 in Section 5.3.2.15. All valid MKPDUs that meet the requirements as defined under FCS_MKA_EXT.1.8 are decoded in a manner conformant to IEEE 802.1x-2010 Section 11.11.4.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

### FCS\_MKA\_EXT.1.8 Guidance 1

Objective	The evaluator shall verify that the guidance documentation provides instructions on how to configure the TOE to act as the Key Server in an environment with multiple MACsec-capable devices.
Evaluator Findings	The evaluator verified that instructions for configuring the TOE to act as the Key Server in an environment with multiple MACsec-capable devices is documented in the TOE guidance documentation. The section titled ‘Configuring MACsec’ of the AGD was used to determine the verdict of this assurance activity. This section provides an external document reference

	<p>[5] which directs the reader to the <a href="#">System Security Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.3.x</a>. Under “Configure MACsec” &amp; “Creating a User-Defined MACsec Policy”, proper guidance has provided to configure key server priority for the TOE.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

## 8 TSS and Guidance Activities (SSH)

### 8.1.1 FCS\_SSHS\_EXT.1

#### FCS\_SSHS\_EXT.1.2 TSS 1

Objective	<p>The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims).</p> <p>The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client’s presented public key matches one that is stored within the SSH server’s authorized_keys file.</p> <p>If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS.</p> <p>TD0631 applied.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, and that this list is consistent with signature verification algorithms selected in FCS_COP.1/SigGen. Upon investigation, the evaluator found that FCS_COP.1.1/SigGen claims <b>RSA</b> as the digital signature mechanism and the TSS states that:</p> <p>SSHv2 is implemented according to the following RFCs: 4251, 4252, 4253, 4254, 4344 and 6668. The TOE implementation of SSHv2 supports the following:</p> <ul style="list-style-type: none"> <li>• Public key algorithms for authentication: RSA Signature Verification.</li> <li>• The TOE allows public key based authentication for remote administrative users: SSH client’s presented public key matches one that is stored within the TOE’s authorized_keys file.</li> <li>• Local password-based authentication for administrative users accessing the TOE through SSHv2.</li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FCS\_SSHS\_EXT.1.3 TSS 1

Objective	The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.
Evaluator Findings	The evaluator examined the section 6.1 titled TOE Summary Specification in the Security Target to verify that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled. Upon investigation, the evaluator found that the TSS states that:  Packets greater than 65,535 bytes in an SSH transport connection are dropped. Large packets are detected by the SSH implementation, and dropped internal to the SSH process.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

### FCS\_SSHS\_EXT.1.4 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.
Evaluator Findings	The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS specifies the optional characteristics and the encryption algorithms supported. Upon investigation, the evaluator found that the TSS states that:  The TOE implementation of SSHv2 supports encryption algorithms, AES128-CTR, AES256-CTR to ensure confidentiality of the session.  Next, the evaluator examined the definition of FCS_SSHS_EXT.1 in ST. The evaluator found that the symmetric encryption specified in the definition of the SFR are consistent with the description within the TSS of ST. Also, no optional SSH characteristics are supported by the TOE.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

### FCS\_SSHS\_EXT.1.4 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	The evaluator examined the section 3.3.1 titled “Remote Administration Protocols” in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that:  IOS XR only supports SSHv2 with the following by default. <ul style="list-style-type: none"> <li>• encryption algorithms, aes128-ctr, aes256-ctr to ensure confidentiality of the session.</li> </ul> Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass.
---------	-------

### FCS\_SSHS\_EXT.1.5 TSS 1

Objective	<p>The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the SSH server's host public key algorithms supported are specified and that they are identical to those listed for this component.</p> <p>TD0631 applied.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS specifies the SSH server's host public key algorithms supported. Upon investigation, the evaluator found that the FCS_SSHS_EXT.1.5 has selection for <b>ssh-rsa</b> and the TSS states that:</p> <p>SSHv2 is implemented according to the following RFCs: 4251, 4252, 4253, 4254, 4344 and 6668. The TOE implementation of SSHv2 supports the following:</p> <ul style="list-style-type: none"> <li>Public key algorithms for authentication: RSA Signature Verification.</li> </ul> <p>The evaluator found that the SSH server's host public algorithm specified in the definition of the SFR are consistent with the description within the TSS of ST.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FCS\_SSHS\_EXT.1.5 Guidance 1

Objective	<p>The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).</p>
Evaluator Findings	<p>The evaluator examined the section 3.3.1 titled "Remote Administration Protocols" in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that:</p> <p>IOS XR only supports SSHv2 with the following by default.</p> <ul style="list-style-type: none"> <li>SSH transport implementation public key algorithms: ssh-rsa.</li> </ul> <p>Also, Section 3.3.1.1 "SSH public-key based authentication" describes the detailed steps to configure the public key for SSH user authentication</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FCS\_SSHS\_EXT.1.6 TSS 1

Objective	<p>The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> in the Security Target to verify that the TSS lists the supported data integrity algorithms, and that that list</p>

	<p>corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE's implementation of SSHv2 supports hashing algorithm hmac-sha1, hmac-sha2-256, and hmac-sha2-512 to ensure the integrity of the session.</p> <p>The evaluator found that the data integrity algorithms specified in the definition of the SFR are consistent with the description within the TSS of the ST.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FCS\_SSHS\_EXT.1.6 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed).
Evaluator Findings	<p>The evaluator examined the section 3.3.1 titled "Remote Administration Protocols" in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD states that:</p> <p>IOS XR only supports SSHv2 with the following by default.</p> <ul style="list-style-type: none"> <li>• encryption algorithms, aes128-ctr, aes256-ctr to ensure confidentiality of the session.</li> <li>• hashing algorithms hmac-sha1, hmac-sha2-256 and hmac-sha2-512 to ensure the integrity of the session.</li> <li>• SSH transport implementation public key algorithms: ssh-rsa.</li> <li>• Key Exchange Algorithms: diffie-hellman-group14-sha1</li> </ul> <p>The evaluator also verified that "none" MAC algorithm is not mentioned in the supported list.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FCS\_SSHS\_EXT.1.7 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> in the Security Target to verify that the TSS lists the supported key exchange algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE's implementation of SSHv2 can be configured to only allow Diffie-Hellman Group 14 (2048-bit keys) Key Establishment, as required by the PP.</b></p>

	<p>The evaluator found that the key exchange algorithms specified in the definition of the SFR are consistent with the description within the TSS of the ST.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FCS\_SSHS\_EXT.1.7 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.
Evaluator Findings	<p>The evaluator examined the section 3.3.1 titled “Remote Administration Protocols” in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD states that:</p> <p>To configure key-exchange algorithms</p> <pre>RP/0/RP0/CPU0: router(config)#ssh server algorithms key-exchange diffie-hellman-group14-sha1</pre> <pre>RP/0/RP0/CPU0: router(config)#commit</pre> <pre>RP/0/RSP0/CPU0: router #crypto key gen rsa</pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FCS\_SSHS\_EXT.1.8 TSS 1

Objective	<p>The evaluator shall check that the TSS specifies the following:</p> <ol style="list-style-type: none"> <li>Both thresholds are checked by the TOE.</li> <li>Rekeying is performed upon reaching the threshold that is hit first.</li> </ol>
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> in the Security Target to verify that the TSS specifies that both thresholds are checked and that rekeying is performed upon reaching the threshold that is hit first. Upon investigation, the evaluator found that the TSS states that :</p> <ul style="list-style-type: none"> <li>The TOE can also be configured to ensure that SSH re-key of no longer than one hour and no more than one gigabyte of transmitted data for the session key.</li> <li>Rekeying is performed upon reaching the threshold that is hit first.</li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FCS\_SSHS\_EXT.1.8 Guidance 1

Objective	If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the guidance documentation describes how to configure those
-----------	---



	<p>thresholds. Either the allowed values are specified in the guidance documentation and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR. The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached.</p>
Evaluator Findings	<p>The evaluator examined the section 3.3.1 titled "Remote Administration Protocols" in the AGD to verify that it describes how to configure any thresholds that are configurable. Upon investigation, the evaluator found that the AGD states that:</p> <p>The "ssh server rekey-time &lt;minutes&gt;" and "ssh server rekey-volume &lt;data in megabytes&gt;" commands configure the SSH rekey to a limit of 60 minutes and 1024MB of data. Based on time the administrator will need to wait for 60 minutes before the rekey occurs. The TOE will begin re-key based upon the first threshold reached.</p> <pre>RP/0/RP0/CPU0: router# (config)#ssh time-out 60</pre> <pre>RP/0/RP0/CPU0: router# (config)#ssh server rekey-time 60</pre> <pre>RP/0/RP0/CPU0: router# (config)#ssh server rekey-volume 1024</pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

## 9 TSS and Guidance Activities (TLS)

### 9.1.1 FCS\_TLSC\_EXT.1

#### FCS\_TLSC\_EXT.1.1 TSS 1

Objective	<p>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.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> 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 <b>TLS is used to protect the TLS sessions with the TOE, which supports the mandatory ciphersuite as well as the following optional ciphersuite:</b></p> <ul style="list-style-type: none"> <li>• <b>TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268</b></li> <li>• <b>TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268</b></li> </ul> <p>Next, the evaluator examined the definition of FCS_TLSC_EXT.1 in ST. The evaluator found that the ciphersuites specified in the definition of the SFR are consistent with the description within the TSS of ST.</p>

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

#### 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	<p>The evaluator examined the section 3.3.4 titled “Logging to Syslog Server via TLS” 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 states that <b>Using a secure TLS connection for Syslog Server is required in the evaluated configuration:</b></p> <pre>RP/0/RP0/CPU0: router #conf RP/0/RP0/CPU0: router (config)#logging tls-server syslog server name RP/0/RP0/CPU0: router (config-logging-tls-peer)# severity debugging RP/0/RP0/CPU0: router (config-logging-tls-peer)# tls-hostname xyz.cisco.com RP/0/RP0/CPU0: router (config-logging-tls-peer)# commit</pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> 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 <b>The TOE requires Subject Alternative Names (SANs) “the reference identifiers” for a successful connection. SANs contain one or more alternate names and uses any variety of name forms for the entity that is bound by the Certificate Authority (CA) to the certified public key. These alternate names are called “Subject Alternative Names” (SANs). Possible names include:</b></p> <ul style="list-style-type: none"> <li>• <b>DNS name.</b></li> </ul> <p><b>Using IP addresses and wildcards is not supported in identity certificates.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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	<p>The evaluator examined the section 6.1 titled TOE SUMMARY SPECIFICATION in the Security Target to verify that, if IP addresses are supported in the CN as reference identifiers. Upon investigation, the evaluator found that the TSS states that:</p> <p>Using IP addresses and wildcards is not supported in identity certificates.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 3.3 titled “X509 Certificates” &amp; “Logging to syslog server via TLS” 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 states that :</p> <p>For secure syslog, the remote server must be authenticated via a trustpoint configuration. First an authorized administrator must configure a hostname and IP domain on the router.</p> <p>The router supports Subject Alternative Name (SAN) and Common Name (CN) with precedence for SAN reference identifiers for a successful connection. The Domain Name system (DNS) name in the SAN is used to match to the configured reference identifier.</p> <pre> logging to the syslog server via TLS needs to be setup. RP/0/RP0/CPU0: router #conf RP/0/RP0/CPU0: router (config)#<b>logging tls-server</b> syslog server name RP/0/RP0/CPU0: router (config-logging-tls-peer)# <b>severity debugging</b> RP/0/RP0/CPU0: router (config-logging-tls-peer)# <b>tls-hostname</b> xyz.cisco.com RP/0/RP0/CPU0: router (config-logging-tls-peer)# <b>commit</b> </pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass.
---------	-------

### 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 behaviour is performed by default or may be configured.
Evaluator Findings	The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> in the Security Target to verify that the TSS describes the Supported Elliptic Curves Extension and whether the required behaviour is performed by default or may be configured. Upon investigation, the evaluator found that the TSS states that:  The TOE does not support NIST Curves in the TLS Client Hello..  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

### 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	TOE does not support any NIST curve.
Verdict	Pass.

## 10 TSS and Guidance Activities (Identification and Authentication)

### 10.1.1 FIA\_AFL.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 section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> 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 TOE provides the privileged administrator the ability to specify the maximum number of unsuccessful authentication attempts before privileged administrator or non-privileged administrator is locked out through the administrative CLI using a privileged CLI command.

	<p>While the TOE supports a range from 1-24, in the evaluated configuration, the maximum number of failed attempts is recommended to be set to 3.</p> <p>Once the remote user is locked out, their account will not be accessible until the configured timer for lockout has been exceeded. Once the lockout time is over, then the administrator user can attempt to login again.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> 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 :</p> <p>At no point is administrator access completely unavailable when remote administrators are locked out due to unsuccessful password attempts. Local console access is always available. Administrator lockouts are not applicable to the local console.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 3.2.8 titled “User Lockout” 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 that:</p> <p>User accounts must be configured to lockout after a specified number of authentication failures.</p> <p style="text-align: center;">RP/O/RP0/CPU0: router(config)#aaa password-policy policy</p>

	<p>RP/0/RP0/CPU0: router(config-pp)#<b>authen-max-attempts 5</b></p> <p>RP/0/RP0/CPU0: router(config-pp)#<b>lockout-time minutes 1</b></p> <p>RP/0/RP0/CPU0: router(config)#<b>username test1 15</b></p> <p>RP/0/RP0/CPU0: router(config-un)#<b>password-policy policy password passwordtest123</b></p> <p>RP/0/RP0/CPU0: router(config-un)#<b>commit</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 3.2.8 titled “User Lockout” 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 the AGD states that:</p> <p><b>Note:</b> Administrator lockouts are not applicable to the local console. Local administrators cannot be locked out and have the ability to unlock other users by using the local console.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 10.1.2 FIA\_AFL.1/MACsec

#### FIA\_AFL.1/MACsec Guidance 1

Objective	The evaluator shall also examine the operational guidance to ensure that instructions for configuring the authentication failure threshold and the TOE’s response to the threshold being met (if configurable), 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 trusted path used to access the TSF (see FTP_TRP.1), all must be described.
Evaluator Findings	The evaluator examined the section 3.2.8 titled “User Lockout” in the AGD to verify that, if the TOE requires configuration to be put into a state where authentication attempt limiting is enforced, it describes the procedures to configure the TOE into this state. Upon investigation, the evaluator found that the AGD states that:

	<p>User accounts must be configured to lockout after a specified number of authentication failures.</p> <pre>RP/0/RP0/CPU0: router(config)#aaa password-policy policy</pre> <pre>RP/0/RP0/CPU0: router(config-pp)#authen-max-attempts 5</pre> <pre>RP/0/RP0/CPU0: router(config-pp)#lockout-time minutes 1</pre> <pre>RP/0/RP0/CPU0: router(config)#username test1 15</pre> <pre>RP/0/RP0/CPU0: router(config-un)#password-policy policy password passwordtest123</pre> <pre>RP/0/RP0/CPU0: router(config-un)#commit</pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 10.1.3 FIA\_PMG\_EXT.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 characters supported for administrator passwords.
Evaluator Findings	<p>The evaluator examined the section 6.1 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 characters supported for administrator passwords. Upon investigation, the evaluator found that the TSS states that:</p> <p>The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “)”. Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 15 characters or greater.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### FIA\_PMG\_EXT.1.1 Guidance 1

Objective	<p>The evaluator shall examine the guidance documentation to determine that it:</p> <ol style="list-style-type: none"> <li>identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and</li> <li>provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.</li> </ol>
Evaluator Findings	The evaluator examined the section section 4.2 titled “Passwords” 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

	<p>the minimum password length and describes the valid minimum password lengths supported. Upon investigation, the evaluator found that the AGD states that:</p> <p>For the evaluated configuration passwords must be a minimum length of 15 characters and composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, “), [no other characters];</p> <p style="text-align: center;">RP/0/RSP0/CPU0: router# <b>configure</b></p> <p style="text-align: center;">RP/0/RSP0/CPU0: router(config)#<b>aaa password-policy policy</b></p> <p style="text-align: center;">RP/0/RSP0/CPU0: router(config)#<b>min-length 15</b></p> <p>To store the passwords securely please use one of the following in order to make the password unreadable:</p> <p style="text-align: center;">RP/0/RSP0/CPU0:router(config-un)# &lt;secret 5   password 9&gt;</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 10.1.4 FIA\_PSK\_EXT.1/MACsec

##### FIA\_PSK\_EXT.1/MACsec TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1. Upon investigation, the evaluator found that the TSS states that: The TOE supports use of pre-shared keys for MACsec key agreement protocols. The pre-shared keys are not generated by the TOE but the TOE accepts the keys in the form of HEX strings. This is done via the CLI configuration command – “key chain test_key macsec.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

##### FIA\_PSK\_EXT.1/MACsec Guidance 1

Objective	The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on the composition of strong pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the range of lengths supported.
-----------	---



Evaluator Findings	<p>The evaluator examined the section 3.3.5 titled “Configuring MACsec” in the AGD which directs the reader to the <a href="#">System Security Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.3.x</a> Under <u>Contents &gt; Configure MACsec &gt; Creating a MACsec key chain</u>, in the section “Creating a MACsec key chain” the appropriate guidance can be found. The evaluator found that the AGD provided instructions on configuring the TOE to accept bit-based keys, using the CLI.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### FIA\_PSK\_EXT.1/MACsec Guidance 2

Objective	The evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both).
Evaluator Findings	<p>The evaluator examined the section 3.3.5 titled “Configuring MACsec” in the AGD which directs the reader to the <a href="#">System Security Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.3.x</a> Under <u>Contents &gt; Configure MACsec &gt; Creating a MACsec key chain</u>, in the section “Creating a MACsec key chain” the appropriate guidance can be found. The evaluator found that the AGD provided instructions on configuring the TOE to accept bit-based keys, using the CLI</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

### 10.1.5 FIA\_UIA\_EXT.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	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> 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:</p> <p>Administrative access to the TOE is facilitated through the TOE’s CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE through either a directly connected console or remotely through an SSHv2 secured connection, the TOE prompts the user for a username and password. Only after the administrative user presents the correct authentication credentials will access to the</p>

	<p>TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated.</p> <p>The TOE provides a local password-based authentication mechanism for authentication of authorized administrators.</p> <p>The process for authentication is the same for administrative access whether administration is occurring via a directly connected console or remotely via SSHv2 secured connection.</p> <p>At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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	<p>The evaluator examined the section 6.1 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:</p> <p>The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for the login warning banner that is displayed prior to user authentication.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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	<p>The evaluator examined the operational guidance to determine that any necessary preparatory steps to logging in are described. Several relevant sections were used to determine the verdict of this assurance activity. The evaluator found that the AGD provides instructions for configuring user authentication on the TOE in the following sections:</p> <ul style="list-style-type: none"> <li>• Section “Initial Setup via Direct Console Connection”</li> <li>• Section “Remote Administration Protocols”</li> <li>• Section “User Roles”</li> <li>• Section “Passwords”</li> </ul> <p>Authentication may be configured via CLI. The instructions provided by AGD place the TOE in a configuration that requires authentication for all administrative access.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 10.1.6 FIA\_UAU.7

#### 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	<p>The evaluator examined the section 3 titled ‘Secure Installation and Configurations’ in the AGD to verify that it describes any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed. Upon investigation, the evaluator found that the AGD states that:</p> <p>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.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 10.1.7 FIA\_X509\_EXT.1/Rev

#### 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 section 6.1 titled <b>TOE Summary Specification</b> 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

	<p>that they are trivially satisfied). Upon investigation, the evaluator found that the TSS states that:</p> <ul style="list-style-type: none"> <li>• The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections</li> <li>• The certificate validation checking takes place during the TLS session establishment and at time of import. The TOE conforms to standard RFC 5280 for certificate and path validation (i.e., peer certificate checked for expiration, peer certificate checked if signed by a trusted CA in the trust chain, peer certificate checked for unauthorized modification, peer certificate checked for revocation).</li> <li>• Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The local certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted. Only one certificate is imported since the only device is a syslog server, so the TOE chooses this certificate basicConstraints checking is performed at the time of authentication during the connection attempt. If the connection to determine the certificate validity cannot be established, the certificate is not accepted.</li> <li>• When the TOE is able to contact the CRL distribution point for certificate revocation checking, the TOE will reject the TLS session if the remote trust point's (e.g. syslog server's) certificate has been revoked.</li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

FIA\_X509\_EXT.1/Rev TSS 2

Objective	<p>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.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> 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:</p> <p>The administrators can configure a trust chain by importing the CA certificate(s) that signed and issued the server (syslog) certificate. This will tell the TOE which CA certificate(s) to use during the validation process. If the TOE does not find the trusted root CA, the TLS connection to the syslog server will fail. When the TOE is able to contact the CRL distribution point for certificate revocation checking, the TOE will reject the TLS session if the remote trust point's (e.g. syslog server's) certificate has been revoked.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

## FIA\_X509\_EXT.1/Rev Guidance 1

Objective	<p>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.</p>
Evaluator Findings	<p>The evaluator examined the section 3.3.3 titled “X.509 Certificates” 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:</p> <p>For secure syslog, the remote server must be authenticated via a trustpoint configuration. First an authorized administrator must configure a hostname and IP domain on the router.</p> <p>The router requires Subject Alternative Names (SANs) “the reference identifiers” for a successful connection. The Domain Name system (DNS) name in the SAN is used to match to the configured reference identifier in the instructions below.</p> <p>The syslog connection fails if the audit server certificate that does not meet any one of the following criteria:</p> <ul style="list-style-type: none"> <li>• The certificate is not signed by the CA with CA flag set to TRUE.</li> <li>• The certificate is not signed by a trusted CA in the certificate chain.</li> <li>• The certificate Common Name (CN) or Subject Alternative Name (SAN) does not match the expected DNS name(i.e., reference identifier).</li> <li>• The certificate has been revoked or modified.</li> </ul> <p><b>Revocation Mechanism for PKI Certificate Status Checking:</b></p> <p>When the router receives a certificate from a peer, it searches its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL is used. Otherwise, the router downloads the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. If the certificate appears on the CRL, your router cannot accept the certificate and will not authenticate the peer. This is the routers default behavior with no configuration required.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

10.1.8 FIA\_X509\_EXT.2

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	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> 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:</p> <p>The administrators can configure a trust chain by importing the CA certificate(s) that signed and issued the server (syslog) certificate. This will tell the TOE which CA certificate(s) to use during the validation process. If the TOE does not find the trusted root CA, the TLS connection to the syslog server will fail.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

FIA\_X509\_EXT.2 TSS 2

Objective	The evaluator shall examine the TSS to confirm that it describes the behaviour 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	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> in the Security Target to verify that the TSS describes the behaviour 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:</p> <p>If the connection to determine the certificate validity cannot be established, the certificate is not accepted.</p> <p>The administrators can configure a trust chain by importing the CA certificate(s) that signed and issued the server (syslog) certificate. This will tell the TOE which CA certificate(s) to use during the validation process. If the TOE does not find the trusted root CA, the TLS connection to the syslog server will fail. When the TOE is able to contact the CRL distribution point for certificate revocation checking, the TOE will reject the TLS session if the remote trust point's (e.g. syslog server's) certificate has been revoked.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

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. The guidance documentation shall also include any required configuration on the
-----------	---

	<p>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.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section 3.3.2.4 titled “Logging Protection” 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 states that:</p> <p>It is recommended that the implemented syslog server complies with the standards documented in RFC 5424. It is also expected that the software is the current version and is regularly updated with the latest patches.</p> <p>Section 3.3.3 provides instructions once X.509 certificates have been configured.</p> <p>Using a secure TLS connection for Syslog Server is required in the evaluated configuration: The minimum TLS version for use to TLSv1.1 and TLSv1.2 with support for the following ciphers that are available by default in FIPS mode.</p> <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> </ul> <p>The evaluator examined the section 3.3.3 titled “X.509 Certificates” in the AGD. Upon investigation, the evaluator found that the AGD states that:</p> <p>For secure syslog, the remote server must be authenticated via a trustpoint configuration. First an authorized administrator must configure a hostname and IP domain on the router.</p> <p>The router requires Subject Alternative Names (SANs) “the reference identifiers” for a successful connection. The Domain Name system (DNS) name in the SAN is used to match to the configured reference identifier in the instructions below.</p> <p>The syslog connection fails if the audit server certificate that does not meet any one of the following criteria:•</p> <ul style="list-style-type: none"> <li>• The certificate is not signed by the CA with cA flag set to TRUE. •</li> <li>• The certificate is not signed by a trusted CA in the certificate chain. •</li> <li>• The certificate Common Name (CN) or Subject Alternative Name (SAN) does not match the expected DNS name(i.e., reference identifier). •</li> <li>• The certificate has been revoked or modified</li> </ul> <p>The evaluator also confirmed that this section includes all the configuration commands required so that the TOE can use the certificates.</p> <p><b>Revocation Mechanism for PKI Certificate Status Checking:</b></p> <p>When the router receives a certificate from a peer, it searches its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL is used. Otherwise, the router downloads the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to</p>

	<p>ensure that the certificate that the peer sent has not been revoked. If the certificate appears on the CRL, your router cannot accept the certificate and will not authenticate the peer. This is the routers default behavior with no configuration required.</p> <p><b>Note:</b> If the connection cannot be established due to a failure during the validity check of a certificate, then an authorized administrator should check the logs and investigate the reason for failure. The administrator shall ensure that the TOE configuration is correct, and all required steps identified in this guidance document are followed correctly. If the problem persists, contact Cisco Technical Assistance via <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> or 1 800 553-2447.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 10.1.9 FIA\_X509\_EXT.3

#### 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 ST does not select "device-specific information". Therefore, a description is not required.
Verdict	Pass.

#### 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	<p>The evaluator examined the section 3.3.3 titled "X.509 Certificates" 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 states that:</p> <p><b><u>Declaring a Certification Authority and Configuring a Trusted Point</u></b></p> <p style="text-align: center;">RP/0/RSP0/CPU0:router# <b>configure</b></p> <p style="text-align: center;">RP/0/RSP0/CPU0:router(config)# <b>crypto ca trustpoint ca-name</b></p> <p style="text-align: center;">ex. RP/0/RSP0/CPU0:router(config)# <b>crypto ca trustpoint myca</b></p>



Note: The below configures the certificate request so that the router ip address will not be included in the certificate request.

```
RP/0/RSP0/CPU0: router(config-trustp)#ip-address none
```

```
RP/0/RSP0/CPU0: router(config-trustp)#subject-name [x.500 distinguished name]
```

```
RP/0/RSP0/CPU0: router(config-trustp)#subject-name C=2letter  
countryid,O=organisation,CN=contactname_email
```

```
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url CA-URL
```

```
ex.RP/0/RSP0/CPU0:router(config-trustp)#enrollment url  
http://myca.domain.com
```

Note: The below command is optional:

```
RP/0/RSP0/CPU0:router(config-trustp)# query url LDAP-URL
```

```
ex.RP/0/RSP0/CPU0:router(config-trustp)# query url ldap://my-  
ldap.domain.com
```

```
RP/0/RSP0/CPU0: router(config)# commit
```

```
RP/0/RSP0/CPU0: crypto ca authenticate ca-name
```

```
Ex. RP/0/RSP0/CPU0:router# crypto ca authenticate myca
```

```
RP/0/RSP0/CPU0: router(config)# crypto ca enroll ca-name
```

```
ex. RP/0/RSP0/CPU0: router(config)# crypto ca enroll myca
```

**Configuring Certificate Enrollment Using Cut and Paste:**

	<p>All of the certificates include at least the public key and Common Name (CN).</p> <pre>RP/0/RSP0/CPU0:router# <b>configure</b></pre> <pre>RP/0/RSP0/CPU0:router(config)# <b>crypto ca trustpoint ca-name</b></pre> <p>ex. RP/0/RSP0/CPU0:router(config)# <b>crypto ca trustpoint myca</b></p> <pre>RP/0/RSP0/CPU0:router(config-trustp)# <b>enrollment terminal</b></pre> <pre>RP/0/RSP0/CPU0:router(config)# <b>commit</b></pre> <pre>RP/0/RSP0/CPU0:router#<b>crypto ca authenticate ca-name</b></pre> <pre>RP/0/RSP0/CPU0: router(config)# <b>crypto ca enroll ca-name</b></pre> <p>ex. RP/0/RSP0/CPU0: router(config)# <b>crypto ca enroll myca</b></p> <pre>RP/0/RSP0/CPU0:router# crypto ca import ca- name certificate</pre> <p>ex. RP/0/RSP0/CPU0:router# crypto ca import myca certificate</p> <pre>RP/0/RSP0/CPU0: router(config-trustp)#<b>ip-address 10.30.0.110</b></pre> <pre>RP/0/RSP0/CPU0: router(config-trustp)#<b>subject-name C=2letter</b></pre> <p><i>countryid,O=organisation,CN=contactname_email</i></p> <pre>RP/0/RSP0/CPU0: router(config-trustp)#<b>serial-number</b></pre> <pre>RP/0/RSP0/CPU0: router(config-trustp)#<b>enrollment url terminal</b></pre> <pre>RP/0/RSP0/CPU0: router(config-trustp)#<b>enrollment retry count 100</b></pre> <pre>RP/0/RSP0/CPU0: router(config-trustp)#<b>enrollment retry period 1</b></pre> <pre>RP/0/RSP0/CPU0: router(config-trustp)#<b>rsakeypair key-name</b></pre> <pre>RP/0/RSP0/CPU0: router(config-trustp)#<b>commit</b></pre> <pre>RP/0/RSP0/CPU0: router(config-trustp)#<b>end</b></pre> <p>The evaluator also confirmed that the ST author selects “Common Name” field for creating the Certificate Request.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

## 11 TSS and Guidance Activities (Security Management)

### 11.1.1FMT\_MOF.1/ManualUpdate

#### 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	<p>The evaluator examined the section 4.5 titled “Product Updates” 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:</p> <p>Here’s the summary of steps necessary to upgrading the software on the router.</p> <ol style="list-style-type: none"><li>Execute:<ul style="list-style-type: none"><li><b>install add source</b> <i>&lt;ftp or sftp transfer protocol&gt;//user@server:/package_path/ filename1 filename2 ...</i></li></ul></li><li>show install request</li><li>show install repository</li><li>show install inactive</li><li>Execute one of these:<ul style="list-style-type: none"><li><b>install activate</b> <i>package_name</i></li><li><b>install activate id</b> <i>operation_id</i></li></ul></li><li>show install active</li><li>install commit</li></ol> <p>Verification of authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image.</p> <p>The evaluator examined the section 2 titled “Secure Acceptance of the TOE” 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 states that:</p> <p>Once the file is downloaded, the authorized administrator verifies that it was not tampered with by either using a hash utility to verify the SHA512 published hash by comparing the SHA512 published hash that is listed on the Cisco web site.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

## 11.1.2 FMT\_MOF.1/Services

### FMT\_MOF.1/Services TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> in the Security Target. Upon investigation, the evaluator found that the TSS states that :</p> <p>The term “Authorized Administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned.</p> <p>...</p> <p>See FMT_SMF.1 for services the Security Administrator is able to start and stop. Management functionality of the TOE is provided through the TOE CLI.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FMT\_MOF.1/Services Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.																		
Evaluator Findings	<p>The evaluator examined the section 4 titled “Secure Management” in the AGD to verify that it describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed. Upon investigation, the evaluator found that the AGD states that:</p> <p>The lists the services the Security Administrator is able to start and stop.</p> <table border="1"> <thead> <tr> <th>Administrative Activity</th> <th>Method (Command Configuration)</th> <th>Section</th> </tr> </thead> <tbody> <tr> <td>Startup of Audit function</td> <td>logging trap debugging</td> <td>3.3.2</td> </tr> <tr> <td>Shutdown of Audit function</td> <td>no logging trap debugging</td> <td>3.3.2</td> </tr> <tr> <td>Logout</td> <td>Exit</td> <td>3.2.7</td> </tr> <tr> <td>Generating Keys (certificates)</td> <td>crypto key generate rsa</td> <td>3.3.1 3.3.3</td> </tr> <tr> <td>Configuring Login failure threshold</td> <td>authen-max-attempts 5</td> <td>3.2.8</td> </tr> </tbody> </table>	Administrative Activity	Method (Command Configuration)	Section	Startup of Audit function	logging trap debugging	3.3.2	Shutdown of Audit function	no logging trap debugging	3.3.2	Logout	Exit	3.2.7	Generating Keys (certificates)	crypto key generate rsa	3.3.1 3.3.3	Configuring Login failure threshold	authen-max-attempts 5	3.2.8
Administrative Activity	Method (Command Configuration)	Section																	
Startup of Audit function	logging trap debugging	3.3.2																	
Shutdown of Audit function	no logging trap debugging	3.3.2																	
Logout	Exit	3.2.7																	
Generating Keys (certificates)	crypto key generate rsa	3.3.1 3.3.3																	
Configuring Login failure threshold	authen-max-attempts 5	3.2.8																	

	Display system information	Show version	2
	Configuring CAs	crypto ca trustpoint	3.3.3
	Generating CSRs	crypto ca enroll <name>	3.3.3
	Performing Software Updates	A series of CLI commands are provided for performing updates	3.2.5
	Setting the Time	clock set	4.3
	Configuring Admin Timeout	exec-timeout <time>	3.2.6
	Configuring the Audit Server	logging host	3.3.2
	Configuring Access Banner	Banner login	4.4
	Setting Password Length	aaa password-policy policy	4.2
	Configuring SSH	ssh server configurations	3.2.5 3.3.1
	MACsec Configuration	A series of CLI commands are provided for configuration of MACsec	3.3.5
	Based on these findings, this assurance activity is considered satisfied.		
Verdict	Pass.		

### 11.1.3 FMT\_MTD.1/CoreData

#### 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	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> in the Security Target to verify that the TSS identifies administrative functions that are accessible through an interface prior to administrator log-in. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE provides administrative users with a CLI to interact with and manage the security functions of the TOE.</p> <p>The term “Authorized Administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged</p>

	<p>administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned.</p> <p>The TOE provides the ability for Authorized Administrators to access TOE data, such as user accounts and roles, audit data, audit server information, configuration data, security attributes, X.509 certificates, login banners, inactivity timeout values, password complexity setting, TOE updates and session thresholds via the CLI. The TOE restricts the access to manage TSF data that can affect security functions of the TOE to the Authorized Administrator/Security Administrator roles.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> 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:</p> <p>The TOE provides the ability for Authorized Administrators to access TOE data, such as user accounts and roles, audit data, audit server information, configuration data, security attributes, X.509 certificates, login banners, inactivity timeout values, password complexity setting, TOE updates and session thresholds via the CLI. The TOE restricts the access to manage TSF data that can affect security functions of the TOE to the Authorized Administrator/Security Administrator roles.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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 section 4.1 titled User Roles in the 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 AGD states that:

	<p>The TOE provides administrative users with a CLI to interact with and manage the security functions of the TOE.</p> <p>The term “Authorized Administrator” refers to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned.</p> <p>The TOE provides the ability for Authorized Administrators to access TOE data, such as user accounts and roles, audit data, audit server information, configuration data, security attributes login banners, inactivity timeout values, password complexity setting, TOE updates and session thresholds via the CLI. The TOE restricts the access to manage TSF data that can affect security functions of the TOE to the Authorized Administrator/Security Administrator roles.</p> <p>Manual software updates can only be done by the authorized administrator through CLI. These updates include software upgrades. The Security Administrators (a.k.a Authorized Administrators) can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

[FMT\\_MTD.1/CoreData Guidance 2](#)

Objective	<p>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.</p>
Evaluator Findings	<p>The evaluator examined the section 3.3.3 titled “X.509 Certificates” 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:</p> <p><b><u>Declaring a Certification Authority and Configuring a Trusted Point</u></b></p> <p style="text-align: center;">RP/0/RSP0/CPU0:router# <b>configure</b></p>

RP/0/RSP0/CPU0:router(config)# **crypto ca trustpoint** *ca-name*

ex. RP/0/RSP0/CPU0:router(config)# **crypto ca trustpoint** *myca*

Note: The below configures the certificate request so that the router ip address will not be included in the certificate request.

RP/0/RSP0/CPU0: router(config-trustp)#**ip-address** none

RP/0/RSP0/CPU0: router(config-trustp)#**subject-name** [*x.500 distinguished name*]

RP/0/RSP0/CPU0: router(config-trustp)#**subject-name** **C=2letter countryid,O=organisation,CN=contactname\_email**

RP/0/RSP0/CPU0:router(config-trustp)# **enrollment url** *CA-URL*

ex.RP/0/RSP0/CPU0:router(config-trustp)#**enrollment url**  
*http://myca.domain.com*

Note: The below command is optional:

RP/0/RSP0/CPU0:router(config-trustp)# **query url** *LDAP-URL*

ex.RP/0/RSP0/CPU0:router(config-trustp)# **query url** *ldap://my-ldap.domain.com*

RP/0/RSP0/CPU0: router(config)# **commit**

RP/0/RSP0/CPU0: **crypto ca authenticate** *ca-name*

Ex. RP/0/RSP0/CPU0:router# **crypto ca authenticate** *myca*

RP/0/RSP0/CPU0: router(config)# **crypto ca enroll** *ca-name*

ex. RP/0/RSP0/CPU0: router(config)# **crypto ca enroll** *myca*



	<p><b>Configuring Certificate Enrollment Using Cut and Paste:</b></p> <p>All of the certificates include at least the public key and Common Name (CN).</p> <pre>RP/0/RSP0/CPU0:router# <b>configure</b></pre> <pre>RP/0/RSP0/CPU0:router(config)# <b>crypto ca trustpoint</b> <i>ca-name</i></pre> <p>ex. RP/0/RSP0/CPU0:router(config)# <b>crypto ca trustpoint</b> <i>myca</i></p> <pre>RP/0/RSP0/CPU0:router(config-trustp)# <b>enrollment terminal</b></pre> <pre>RP/0/RSP0/CPU0:router(config)# <b>commit</b></pre> <p>The evaluator examined the section 3.3.3 titled “X.509 Certificates” 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 that:</p> <p>Below command is used to authenticate certificates:</p> <pre>RP/0/RSP0/CPU0:router#crypto ca authenticate <i>ca-name</i></pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 11.1.4 FMT\_MTD.1/CryptoKeys

#### FMT\_MTD.1/CryptoKeys TSS 2

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 FCS_CKM.1, FCS_CKM.4 and 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 TOE implements DH group 14 key establishment schemes that meets RFC 3526, Section 3 and RFC7919. The TOE acts as both a sender and receiver for Diffie-Helman based key establishment schemes.

The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP 800-56A and with section 6.

The TOE can create an RSA public-private key pair, with a minimum RSA key size of 2048-bit.

RSA scheme can be used to generate a Certificate Signing Request (CSR). Via offline CSR or Simple Certificate Enrollment Protocol (SCEP), the TOE can: send the CSR to a Certificate Authority (CA) for the CA to generate a certificate; and receive its X.509 certificate from the CA. Integrity of the CSR and certificate during transit are assured through use of digital signatures (encrypting the hash of the TOE's public key contained in the CSR and certificate). The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). The IOS-XR Software supports embedded PKI client functions that provide secure mechanisms for distributing, managing, and revoking certificates. The TOE can also use X.509v3 certificates for authentication of TLS sessions.

The TOE acts as both a sender and receiver for RSA-based key establishment schemes. The RSA key establishment meets the RSAES-PKCS1-v1\_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.

Scheme	SFR	Service
RSA Key generation Key establishment	FCS_SSHS_EXT.1	SSH Remote Administration
	FCS_TLSC_EXT.1	Support for SSH and TLS key establishment
FFC Key generation Key establishment	FCS_SSHS_EXT.1	SSH Remote Administration
	FIA_X509_EXT.1/Rev FIA_X509_EXT.2 FIA_X509_EXT.3	Transmit generated audit data to an external IT entity

The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) when no longer required for use.

See Table 19: TOE Key Zeroization in Section 7 Key Zeroization. The information provided in the table includes all of the all secrets, keys and associated values, the description, and the method used to zeroization when no longer required for use.

	<p>The information is provided in the reference section for ease and readability of all of the all secrets, keys and associated values, their description and zeroization methods.</p> <p>The evaluator also verified that the TSS states how the administrator performs operations on the cryptographic keys. The TSS states:</p> <p>The TOE provides the ability for Authorized Administrators to access TOE data, such as user accounts and roles, audit data, audit server information, configuration data, security attributes, X.509 certificates, login banners, inactivity timeout values, password complexity setting, TOE updates and session thresholds via the CLI. The TOE restricts the access to manage TSF data that can affect security functions of the TOE to the Authorized Administrator/Security Administrator roles.</p> <p>The Security Administrator is able to manage the cryptographic keys (generating keys, importing keys, or deleting keys) that are used in TLS and SSH communications. These keys can be managed via CLI as part of following operations:</p> <ul style="list-style-type: none"> <li>• TLS public/private keys – CSR (keypair) generation, certificate import/export, Trust store management</li> <li>• TLS/SSH session keys– as part of session establishment and termination</li> <li>• SSH public/private keys – generate keypair, import/export public keys, public key-based authentication</li> <li>• MACsec keys – as part of MACsec session establishment and termination</li> <li>• Zeroize – delete keys</li> </ul> <p>The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) when no longer required for use.</p> <p>See Table 19: TOE Key Zeroization in Section 7 Key Zeroization. The information provided in the table includes all of the all secrets, keys and associated values, the description, and the method used to zeroization when no longer required for use. Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FMT\_MTD.1/CryptoKeys Guidance 2

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 3.2.5 titled “Enabling FIPS mode” 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:

	<p>The evaluator found that the AGD has instructions to generate/modify/delete the crypto keys.</p> <ul style="list-style-type: none"> <li>• Generate the crypto key for SSH using the “<b>crypto key generate rsa</b>” command.</li> <li>• Generate RSA key material – choose a longer modulus length for more secure keys (i.e. 2048 for RSA):  RP/0/RSP0/CPU0:router# <b>crypto key generate rsa general-keys rsa</b>    RP/0/RSP0/CPU0:router# How many bits in the modulus [512]: <b>2048</b>    RP/0/RSP0/CPU0:router#<b>show crypto key mypubkey rsa</b></li> </ul> <ul style="list-style-type: none"> <li>• To delete an RSA key from the router, use the crypto key zeroize rsa command in XR EXEC mode.    RP/0/RP0/CPU0: router# <b>crypto key zeroize rsa</b></li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 11.1.5 FMT\_SMF.1

#### FMT\_SMF.1 TSS 1

Objective	<p>The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface).</p> <p>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.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> in the TSS to verify that it details which security management functions are available through which interface(s). Upon investigation, the evaluator confirmed that the management functions specified in FMT_SMF.1 are provided by the TOE. The entirety of the TSS, Guidance Documentation and the TOE (as observed during testing) were used to determine the verdict for this activity. Upon investigation, the evaluator found that the TOE provides the management functions specified in FMT_SMF.1 are available via local (console) and remote (SSH) interface via CLI. The TSS states:</p> <p>The TOE provides all the capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The specific management capabilities available from the TOE include -</p>

- Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described below;
  - The ability to manage the warning banner message and content – allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users)
  - The ability to manage the time limits of session inactivity which allows the Authorized Administrator the ability to set and modify the inactivity time threshold.
  - The ability to update the IOS-XR software. The validity of the image is provided using digital signature or hash comparison prior to installing the update
  - The ability to manage audit behavior and the audit logs which allows the Authorized Administrator to configure the audit logs, view the audit logs, and to clear the audit logs
  - The ability to display the log on banner and to allow any network packets as configured by the authorized administrator may flow through the router prior to the identification and authentication process
  - The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2
  - The ability to configure the authentication failure parameters for FIA\_AFL.1.
  - The ability to configure the cryptographic functionality.
  - The ability to configure thresholds for SSH rekeying.
  - The ability to set the time which is used for time-stamps.
  - The ability to configure the reference identifier for the peer.
  - Ability to import X.509v3 certificates to the TOE’s trusted store.
  - Ability to manage the trusted public keys database.
  - Ability to configure the time interval for administrator lockout due to excessive authentication failures.
- 
- The ability of the Security Administrator to:
    - Generate a PSK-based CAK and install it in the device
    - Manage the Key Server to create, delete, and activate MKA participants [as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XKeyMkaParticipantEntry) and section 12.2 (cf. function createMKA())];
    - Specify a lifetime of a CAK;
    - Enable, disable, or delete a PSK-based CAK using [CLI management command]
    - Configure the number of failed administrator authentication attempts that will cause an account to be locked out
    - Ability to start and stop services

The evaluator examined the section titled “Operational Environment” in the AGD to verify that they describe the local administrative interface. Section 3 of the AGD also states that “Secure Management – provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection.”.

	<p>The evaluator ensured that the Guidance Documentation clearly mentions “local console” or “console” to identify and ensure that the interface is local and includes appropriate warnings for the administrator where applicable such as:</p> <p><b>Note:</b> Administrator lockouts are not applicable to the local console. Local administrators cannot be locked out and have the ability to unlock other users by using the local console.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

[FMT\\_SMF.1.1/MACsec TSS 1 \[TD0652\]](#)

Objective	<p>The evaluator shall verify that the TSS describes the ability of the TOE to provide the management functions defined in this SFR in addition to the management functions required by the base NDcPP.</p> <p>TD0652 applied.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes the ability of the TOE to provide the management functions defined in this SFR in addition to the management functions required by the base NDcPP. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE provides all the capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The specific management capabilities available from the TOE include -</p> <ul style="list-style-type: none"> <li>• Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above;</li> <li>• The ability to manage the warning banner message and content – allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users</li> <li>• The ability to manage the time limits of session inactivity which allows the Authorized Administrator the ability to set and modify the inactivity time threshold.</li> <li>• The ability to update the IOS-XR software. The validity of the image is provided using digital signature or hash comparison prior to installing the update</li> <li>• The ability to manage audit behavior and the audit logs which allows the Authorized Administrator to configure the audit logs, view the audit logs, and to clear the audit logs</li> <li>• The ability to display the log on banner and to allow any network packets as configured by the authorized administrator may flow through the router prior to the identification and authentication process</li> <li>• The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2</li> <li>• The ability to configure the authentication failure parameters for FIA_AFL.1.</li> <li>• The ability to configure the cryptographic functionality.</li> <li>• The ability to configure thresholds for SSH rekeying.</li> <li>• The ability to set the time which is used for time-stamps.</li> <li>• The ability to configure the reference identifier for the peer.</li> </ul>

	<ul style="list-style-type: none"> <li>• Ability to import X.509v3 certificates to the TOE's trusted store.</li> <li>• Ability to manage the trusted public keys database.</li> </ul> <p>The ability of the Security Administrator to:</p> <ul style="list-style-type: none"> <li>• Generate a PSK-based CAK and install it in the device</li> <li>• Manage the Key Server to create, delete, and activate MKA participants [as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipantEntry) and section 12.2 (cf. function createMKA());</li> <li>• Specify a lifetime of a CAK;</li> <li>• Enable, disable, or delete a PSK-based CAK using [CLI management command]</li> <li>• Configure the number of failed administrator authentication attempts that will cause an account to be locked out</li> <li>• Ability to start and stop services</li> <li>• <u>Configure the time interval for administrator lockout due to excessive authentication failures;</u></li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

### FMT\_SMF.1/MACsec Guidance 1

Objective	<p>The evaluator shall examine the operational guidance to determine that it provides instructions on how to perform each of the management functions defined in this SFR in addition to those required by the base NDcPP.</p> <p>TD0652 applied.</p>
Evaluator Findings	<p>The evaluator examined the following sections in the AGD to verify that it provides instructions on how to perform each of the management functions defined in this SFR in addition to those required by the base NDcPP. Upon investigation, the evaluator mentioned the respective sections in the AGD for the points stated in the SFR as below:</p> <p><b>The specific management capabilities available from the TOE include:</b></p> <ul style="list-style-type: none"> <li>• <b>Ability to administer the TOE locally and remotely;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Initial Setup via Direct Console Connection'</i></li> <li>○ <i>Section 'Remote Administration Protocols'</i></li> </ul> </li> <li>• <b>Ability to configure the access banner;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Login Banners'</i></li> </ul> </li> <li>• <b>Ability to configure the session inactivity time before session termination or locking;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Session Termination'</i></li> </ul> </li> <li>• <b>Ability to update the TOE, and to verify the updates using digital signature and [hash comparison] capability prior to installing those updates;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Secure Acceptance of the TOE'</i></li> <li>○ <i>Section 'Product Updates'</i></li> </ul> </li> <li>• <b>Ability to configure the authentication failure parameters for FIA_AFL.1;</b></li> </ul>

	<ul style="list-style-type: none"> <li>○ <i>Section 'User Lockout'</i></li> <li>● <b>Ability of a Security Administrator to Generate a PSK-based CAK and install it in the device</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Configuring MACsec'</i></li> </ul> </li> <li>● <b>Ability of a Security Administrator to Manage the Key Server to create, delete, and activate MKA participants [as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipantEntry) and section. 12.2 (cf. function createMKA())];</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Configuring MACsec'</i></li> </ul> </li> <li>● <b>Ability of a Security Administrator to Specify a lifetime of a CAK</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Configuring MACsec'</i></li> </ul> </li> <li>● <b>Ability of a Security Administrator to Enable, disable, or delete a PSK-based CAK using [[CLI management commands]]</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Configuring MACsec'</i></li> </ul> </li> <li>● <b><u>Configure the time interval for administrator lockout due to excessive authentication failures</u></b> <ul style="list-style-type: none"> <li>○ <i>Section 'User Lockout'</i></li> </ul> </li> <li>● <b>Ability of a Security Administrator to Configure the number of failed administrator authentication attempts that will cause an account to be locked out;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'User Lockout'</i></li> </ul> </li> <li>● <b>Ability to start and stop services;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Initial Setup via Direct Console Connection'</i></li> </ul> </li> <li>● <b>Ability to configure audit behavior (e.g. changes to storage locations for audit; changes to behavior when local audit storage space is full);</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Logging Configuration'</i></li> </ul> </li> <li>● <b>Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Secure Management'</i></li> </ul> </li> <li>● <b>Ability to configure the cryptographic functionality;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Remote Administration Protocols'</i></li> </ul> </li> <li>● <b>Ability to configure thresholds for SSH rekeying;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Remote Administration Protocols'</i></li> </ul> </li> <li>● <b>Ability to set the time which is used for time-stamps;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Clock Management'</i></li> </ul> </li> <li>● <b>Ability to configure the reference identifier for the peer;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'X.509 Certificates'</i></li> </ul> </li> <li>● <b>Ability to import X.509v3 certificates to the TOE's trust store;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'X.509 Certificates'</i></li> </ul> </li> <li>● <b>Ability to manage the trusted public keys database;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'X.509 Certificates'</i></li> </ul> </li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.



## 11.1.6 FMT\_SMR.2

### 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	<p>The evaluator examined the section 6.1 titled <b>TOE SUMMARY SPECIFICATION</b> in the TSS and the section 4.1 titled “User Roles” 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 AGD states that:</p> <p>The TOE platform maintains both privileged and semi-privileged administrator roles. The terms “Authorized Administrator” and "Security Administrator" are used interchangeable in this ST to refer to any user that has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. The assigned role determines the functions the user can perform; hence the authorized administrator with the appropriate privileges.</p> <p>The TOE supports both local administration via a directly connected console cable and remote administration via SSH.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 3.3 titled “Initial Setup via Direct Console Connection” 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 states that:</p> <p>To only allow ssh for remote administrator sessions, use the <b>transport input ssh</b> command.</p> <pre>RP/0/RP0/CPU0: router(config)#line default RP/0/RP0/CPU0: router(config-line)#transport input ssh RP/0/RP0/CPU0: router(config-line)#commit</pre> <p>The evaluator found that the AGD describes the configuration necessary to administer the TOE using the CLI from the following interfaces:</p> <ol style="list-style-type: none"> <li>1. Via Direct console connection – Section Initial Setup via Direct Console Connection</li> <li>2. Via Remote connection using SSH – Section Remote Administration Protocols</li> </ol>

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

## 12 TSS and Guidance Activities (Protection of the TSF)

### 12.1.1 FPT\_APW\_EXT.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	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” 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. Upon investigation, the evaluator found that the TSS states that <b>All passwords are obscured via hashing in a secure directory.</b></p> <p>The evaluator also examined the section <b>6.1</b> titled “<b>TOE Security Functional Requirement Measures</b>” in the Security Target to verify 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:</p> <p><b>All passwords are obscured via hashing in a secure directory. The passwords are non-readable and encrypted. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. This is provided by default.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 12.1.2 FPT\_CAK\_EXT.1

#### FPT\_CAK\_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how CAKs are stored and that they are unable to be viewed through an interface designed specifically for that purpose. If these values are not stored in plaintext, the TSS shall describe how they are protected or obscured.
Evaluator Findings	The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS details how CAKs 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:

	<p>During the setup and configuration of the TOE and the MACsec functionality, the Authorized Administrator issues the command – “password encryption aes”. This prevents the CAK value from being shown in clear text to the administrators on the CLI when the “show run” output is displayed.</p> <p>In addition, CAK data is stored in secure directory that is not readily accessible to administrators.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

### 12.1.3FPT\_FLS.1(2)/SelfTest

#### FPT\_FLS.1(2)/SelfTest TSS 1 [TD0190]

Objective	The evaluator shall examine the TSS to determine that it indicates that the TSF will shut down in the event that a self-test failure is detected. For TOEs with redundant failover capability, the evaluator shall examine the TSS to determine that it indicates that the failed components will shut down in the event that a self-test failure is detected.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS indicates that the TSF will shut down in the event that a self-test failure is detected. Upon investigation, the evaluator found that the TSS states that: Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE. The TOE shuts down by reloading and will continue to reload as long as the failures persist. This functionally prevents any failure of power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests from causing an unauthorized information flow. There are no failures that circumvent this protection.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### FPT\_FLS.1(2)/SelfTest Guidance 1 [TD0190]

Objective	The evaluator shall examine the operational guidance to verify that it describes the behavior of the TOE following a self-test failure and actions that an administrator should take if it occurs.
Evaluator Findings	The evaluator examined the section 3.2.5.3 titled “Self-tests” in the AGD to verify that it describes the behavior of the TOE following a self-test failure and actions that an administrator should take if it occurs. Upon investigation, the evaluator found that the AGD states:

	<p>If any of the POST fail, the following actions should be taken:</p> <ul style="list-style-type: none"> <li>Use the <b>system cores</b> command to set up core dumps on the system. This will provide additional information on the cause of the crash:  RP/0/RP0/CPU0: router# <b>configure</b></li> </ul> <p>RP/0/RP0/CPU0: router(config)# <b>system cores slot0:core_file</b></p> <p>Example:</p> <p>RP/0/RP0/CPU0: router # <b>system cores tftp://x.x.x.x/filename</b></p> <p>RP/0/RP0/CPU0: router # <b>show system cores</b></p> <p>Note: The filename (indicated by filename) must exist in the TFTP server directory.</p> <ul style="list-style-type: none"> <li>Restart the TOE to perform POST and determine if normal operation can be resumed</li> </ul> <p>If the problem persists, contact Cisco Technical Assistance via <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> or 1 800 553-2447</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 12.1.4FPT\_RPL.1

##### FPT\_RPL.1.2 TSS 1

Objective	The evaluator shall examine the TSS to determine that it describes how replay is detected for MPDUs and how replayed MPDUs are handled by the TSF.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” in the Security Target to verify that the TSS describes how replay is detected for MPDUs and how replayed MPDUs are handled by the TSF. Upon investigation, the evaluator found that the TSS states that MPDUs are replay protected in the TOE. Also, the MKA frames are guarded against replay (If a MKPDU with duplicate MN (member number) and not latest MN comes along, then this MKPDU will be dropped and not processed further). Replay data is discarded and logged by the TOE.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 12.1.5FPT\_SKP\_EXT.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	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> 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 <b>The TOE stores all private keys in a secure directory that is not readily accessible to administrators. All pre-shared and symmetric keys are stored in a hashed format that are non-readable, hence no interface access.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 12.1.6FPT\_STM\_EXT.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.
Evaluator Findings	<p>The evaluator examined the section 6.1 titled <b>TOE Summary Specification</b> 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 <b>The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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	<p>The evaluator examined the section 4.3 titled “Clock Management” in the AGD to verify that it instructs the administrator how to set the time. Upon investigation, the evaluator found that the AGD states that:</p> <p>Clock management is restricted to the privileged administrator. Use the clock set command for initial configuration. The ‘clock set’ command updates both SW as well as HW clock.</p> <p>RP/O/RP0/CPU0: router# <b>clock set</b> <i>hh:mm:ss { day month   month day } year</i></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass.
---------	-------

## 12.1.7FPT\_TST\_EXT.1.1

### FPT\_TST\_EXT.1.1 TSS 1

Objective	<p>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.</p>
Evaluator Findings	<p>The TOE is designed to runs the suite of power-on self-tests that comply with the FIPS140-2 requirements for self-test (eg know answer tests (KATs) and zeroization tests), during initial start-up to verify its correct operation. If any of the tests fail the security administrator will have to log into the CLI to determine which test failed and why. If the tests pass successfully the router will continue bootup and normal operation.</p> <p>During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests include:</p> <ul style="list-style-type: none"> <li>• AES Known Answer Test – For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly.</li> <li>• RSA Signature Known Answer Test (both signature/verification) This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.</li> <li>• RNG/DRBG Known Answer Test – For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.</li> <li>• HMAC Known Answer Test –</li> </ul>

	<p>For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly.</p> <ul style="list-style-type: none"> <li>• SHA-1/256 Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly.</li> <li>• Software Integrity Test – The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that’s about to be loaded has maintained its integrity.</li> </ul> <p>If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen, and saved in the crashinfo file.</p> <p>All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic.</p> <p>These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 3.2.5 titled “Self-tests” 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:</p> <p>If any of the POST fail, the following actions should be taken:</p> <ul style="list-style-type: none"> <li>• Use the <b>system cores</b> command to set up core dumps on the system. This will provide additional information on the cause of the crash:  RP/0/RP0/CPU0: router# <b>configure</b>   RP/0/RP0/CPU0: router(config)# <b>system cores slot0:core_file</b>   Example:   RP/0/RP0/CPU0: router # <b>system cores tftp://x.x.x.x/filename</b></li> </ul>

	<p>RP/O/RPO/CPU0: router # <b>show system cores</b></p> <p>Note: The filename (indicated by filename) must exist in the TFTP server directory.</p> <ul style="list-style-type: none"> <li>Restart the TOE to perform POST and determine if normal operation can be resumed</li> </ul> <p>If the problem persists, contact Cisco Technical Assistance via <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> or 1 800 553-2447</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 12.1.8FPT\_TUD\_EXT.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 section 6.1 titled “TOE Security Functional Requirement Measures” 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: An Authorized Administrator can query the software version running on the TOE and can initiate updates to software images.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

#### 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 FPT_TUD_EXT.1 in the 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.



	<p>The evaluator examined the section titled <b>TOE SUMMARY SPECIFICATION</b> 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 :</p> <p>When software updates are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The updates can be downloaded from the software.cisco.com. The cryptographic hashes (i.e., public hashes/SHA-512) are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. Once the file is downloaded from the Cisco.com web site, and upon installation of a TOE update, a digital signature verification check will automatically be performed to ensure it has not been modified since distribution. The authorized source for the digitally signed updates is "Cisco Systems, Inc.".</p> <p>The hash value can be displayed by hovering over the software image name under details on the Cisco.com web site. If the hashes do not match, contact Cisco Technical Assistance Center (TAC).</p> <p>The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded. The digital certificates used by the update verification mechanism are contained on the TOE.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FPT\_TUD\_EXT.1 TSS 5

Objective	<p>If a published hash is used to protect the trusted update mechanism, then the evaluator shall verify that the trusted update mechanism does involve an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. In particular, authentication as Security Administration according to FMT_MOF.1/ManualUpdate needs to be part of the update process when using published hashes.</p>
Evaluator Findings	<p>The evaluator examined the section 6.1 titled "TOE Security Functional Requirement Measures" in the Security Target to verify that the TSS, if a published hash is used to protect the trusted update mechanism, contains a description of how the trusted update mechanism involves an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. Upon investigation, the evaluator found that the TSS states that :</p> <p>Once the file is downloaded from the Cisco.com web site, and upon installation of a TOE update, a digital signature verification check will automatically be performed to ensure it has</p>

	<p>not been modified since distribution. The authorized source for the digitally signed updates is "Cisco Systems, Inc."</p> <p>The hash value can be displayed by hovering over the software image name under details on the Cisco.com web site. If the hashes do not match, contact Cisco Technical Assistance Center (TAC).</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 3.2.2 titled "Boot Verification" 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:</p> <p>To verify the version of IOS-XR use the "<b>show version</b>".</p> <p>Delayed activation is not supported</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section 2 titled "Secure Acceptance of the TOE", "Installing and Activating Packages", and "Product Updates" 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 has proper guidance to verify that they are installed correctly.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>The evaluator examined the section titled “Secure Acceptance of the TOE” in the AGD to verify that it describes, if a published hash is used to protect the trusted update mechanism, how the Security Administrator can obtain authentic published hash values for the updates. Upon investigation, the evaluator found that the AGD states that:</p> <p>The authorized administrator verifies that it was not tampered with by either using a hash utility to verify the SHA512 published hash by comparing the SHA512 published hash that is listed on the Cisco web site and in Section 2 of the AGD. If the hashes do not match, contact Cisco Technical Assistance Center (TAC)  <a href="http://tools.cisco.com/ServiceRequestTool/create/launch.do">http://tools.cisco.com/ServiceRequestTool/create/launch.do</a>.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### FPT\_TUD\_EXT.1 Guidance 6

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	<p>Certificate-based update mechanism is not supported.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

## 13 TSS and Guidance Activities (TOE Access)

### 13.1.1 FTA\_SSL\_EXT.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	<p>The evaluator examined the 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 An administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the “session-timeout” setting applied to the console. When a session is inactive (i.e., no session input from the administrator) for the configured period of time the TOE will terminate the session, and no further activity is allowed requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session.</p> <p>The allowable inactivity timeout range is from 1 to 65535 seconds. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the “exec-timeout” setting.</p>

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

### 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	<p>The evaluator examined the section 3.2.6 titled “Session Termination” 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:</p> <p>Inactivity settings must trigger termination of the administrator session. By default, console, vty, and tty sessions disconnect after 10 minutes of inactivity. Administrators are advised to maintain this value at 10 minutes or less but greater than zero</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 13.1.2 FTA\_SSL.3

#### 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	<p>The evaluator examined the 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 An administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the “session-timeout” setting applied to the console.</p> <p>If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session.</p> <p>The allowable inactivity timeout range is from 1 to 65535 seconds. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the “exec-timeout” setting.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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.
-----------	---

<p>Evaluator Findings</p>	<p>The evaluator examined the section 3.2.6 titled “Session Termination” 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:</p> <p>Inactivity settings must trigger termination of the administrator session. By default, console, vty, and tty sessions disconnect after 10 minutes of inactivity. Administrators are advised to maintain this value at 10 minutes or less but greater than zero. Note: A 0-minute value will prevent sessions from terminating.</p> <p>These settings are configurable as follows:</p> <pre>RP/0/RP0/CPU0: router(config)#<b>vty default 0 4 line-template default</b></pre> <pre>RP/0/RP0/CPU0: router(config)#<b>line default</b></pre> <pre>RP/0/RP0/CPU0: router (config-line)#<b>exec-timeout minutes seconds</b></pre> <pre>RP/0/RP0/CPU0: router(config)#<b>commit</b></pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass.</p>

### 13.1.3 FTA\_SSL.4

#### FTA\_SSL.4 TSS 1

<p>Objective</p>	<p>The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the 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 An administrator is able to exit out of both local and remote administrative sessions. Each administrator logged onto the TOE can manually terminate their session using the “exit” command.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

#### FTA\_SSL.4 Guidance 1

<p>Objective</p>	<p>The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section 3.2.7 titled “Logout” 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 states that:</p> <p>An administrator can manually logout from the evaluated configuration either from the local console or remotely with the following command: <b>exit</b></p>

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

### 13.1.4 FTA\_TAB.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 section titled <b>TOE Summary Specification</b> 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 <b>The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE. This interface is applicable for both local (via console) and remote (via SSH) TOE administration.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

#### 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 4.4 titled “Login Banners” in the AGD to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD states that:  The TOE may be configured by the privileged administrators with banners using the <b>banner motd</b> command. This banner is displayed after the username and before password prompts. To create a banner of text “This is a banner” use the command.  <pre>RP/O/RP0/CPU0: router# <b>configure</b></pre> <pre>RP/O/RP0/CPU0: router(<i>config</i>)# <b>banner motd #Welcome to the C8000 Series#</b></pre> Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

## 14 TSS and Guidance Activities (Trusted Path/Channels)

### 14.1.1 FTP\_ITC.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	<p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” 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:</p> <ul style="list-style-type: none"> <li>• The TOE protects communications with the external audit server using TLS to secure the communications channel.</li> <li>• MACsec is used to secure communication channels between MACsec peers at Layer 2.</li> </ul> <p>The evaluator examined the section 6.1 titled “TOE Security Functional Requirement Measures” 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 following protocols are used to connect to authorized IT entities,</p> <ul style="list-style-type: none"> <li>• TLS</li> <li>• MACsec</li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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 “Logging to Syslog Server via TLS”, “Logging Protection” and “Configuring MACsec” respectively 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 states that:

	<p>contains instructions for establishing the allowed protocols with each authorized IT entity. The allowed protocols are:</p> <ul style="list-style-type: none"> <li>• TLS – Sections ‘Logging to Syslog Server via TLS’ and ‘Logging Protection’</li> <li>• MACsec – Section ‘Configuring MACsec’</li> </ul> <p>Additionally, the AGD states:</p> <p>If any of the established trusted channels/paths are unintentionally broken, the connection will need to be re-established following the configuration settings as described in this document.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 14.1.2 FTP\_TRP.1/Admin

#### 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	<p>The evaluator examined <b>FTP_TRP.1/Admin</b> entry in the section titled <b>TOE Summary Specification</b> 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 <b>All remote administrative communications take place over a secure encrypted SSHv2 session. The SSHv2 session is encrypted using AES encryption.</b></p> <p>The evaluator examined <b>FTP_TRP.1/Admin entry</b> in the section titled <b>TOE Summary Specification</b> 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 remote users are able to initiate SSHv2 communications with the TOE.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 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 3.3.1 titled “Remote Administration Protocol” 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 states that:



	<p>To only allow ssh for remote administrator sessions, use the <b>transport input ssh</b> command.</p> <p>RP/0/RP0/CPU0: router(config)#<b>line default</b></p> <p>RP/0/RP0/CPU0: router(config-line)#<b>transport input ssh</b></p> <p>RP/0/RP0/CPU0: router(config-line)#<b>commit</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

## 15 Detailed Test Cases (Test Activities)

### 15.1.1 Audit

#### FAU\_GEN.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>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&amp;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.</p> <p>Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• The audit records required for this test case can be found in the test cases associated with each of the listed SFRs.</li></ul>
<b>Expected Test Results</b>	<p>The TOE should be able to generate audit records for each of the events described in the ST under the FAU_GEN.1.2.</p> <p>The audit records generated should match the proper format as specified in the guidance documentation.</p>
<b>Pass/Fail with Explanation</b>	<p>Pass, covered by audit records in each test case.</p>

## FAU\_STG\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	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 particular 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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Verify the syslog version.</li> <li>• Configure the TOE for TLS connection.</li> <li>• Configure the server certificate.</li> <li>• Start the TLS connection with supported cipher TLS_RSA_WITH_AES128_SHA.</li> <li>• Verify with the logs.</li> <li>• Verify with the packet capture.</li> <li>• Verify the syslog logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Each configuration change is audited and sent to the audit server</li> <li>• The packet capture is encrypted.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. This test case showed that, when logs are sent from the TOE to the syslog server and the connection is configured to be encrypted. This meets the requirement.

## FAU\_STG\_EXT.1 Test #2 (b)

Item	Data
<b>Test Assurance Activity</b>	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 behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that:

	The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option 'overwrite previous audit records' in FAU_STG_EXT.1.3)
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure smallest possible logging space.</li> <li>• Find the timestamp of the oldest message in the local audit log.</li> <li>• Generate as much audit records which full the logging buffered space.</li> <li>• Verify that the old logs are overwritten.</li> </ul>
<b>Expected Test Results</b>	The TOE should overwrite the logs when the local logging buffered space is full.
<b>Pass/Fail with Explanation</b>	Pass. When audit data is filled to the max, the existing audit data is overwritten. This meets the testing requirement.

### FAU\_STG\_EXT.1 Test #3

Item	Data
<b>Test Assurance Activity</b>	Test 3: If the TOE complies with FAU_STG_EXT.2/LocSpace the evaluator shall verify that the numbers provided by the TOE according to the selection for FAU_STG_EXT.2/LocSpace are correct when performing the tests for FAU_STG_EXT.1.3
<b>Test Steps</b>	NA
<b>Expected Test Results</b>	NA
<b>Pass/Fail with Explanation</b>	NA, The ST does not claim conformance to FAU_STG_EXT.2/LocSpace

## FPT\_STM\_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: If the TOE supports direct <b>setting of the time by the Security Administrator</b> 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	<ul style="list-style-type: none"><li>• Confirm current time (SSH).</li><li>• Set a new time for the TOE.</li><li>• Verify the time on the TOE was updated.</li><li>• Verify logs were generated for time change.</li></ul>
Expected Test Results	The time should change on the TOE set by Security Administrator.
Pass/Fail with Explanation	Pass. The TOE allows the administrative user to configure the time on the TOE. This meets the testing requirements.

## FTP\_ITC.1 Test #1

Item	Data
Test Assurance Activity	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.
Pass/Fail with Explanation	This testing was performed in conjunction with FCS_TLSC_EXT.1.1 Test #1, FAU_STG_EXT.1.1 Test #1 & FCS_MACSEC_EXT.1.1 Test #1. The TOE can be configured to successfully communicate with the external audit server via TLS and with MACsec peer. This meets the testing requirements.

## FTP\_ITC.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Pass/Fail with Explanation</b>	This testing was performed in conjunction with FCS_TLSC_EXT.1.1 Test #1, FAU_STG_EXT.1.1 Test #1 & FCS_MACSEC_EXT.1.1 Test #1. External connections from the TOE are sent via an encrypted channel. This meets the testing requirements

## FTP\_ITC.1 Test #3

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
<b>Pass/Fail with Explanation</b>	This testing was performed in conjunction with FCS_TLSC_EXT.1.1 Test #1, FAU_STG_EXT.1.1 Test #1 & FCS_MACSEC_EXT.1.1 Test #1. External connections from the TOE are sent via an encrypted channel. This meets the testing requirements.

## FTP\_ITC.1 Test #4

Item	Data
<b>Test Assurance Activity</b>	<p>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.</p> <p>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:</p> <ol style="list-style-type: none"><li>1. A duration that exceeds the TOE's application layer timeout setting,</li><li>2. A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer.</li></ol> <p>The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext.</p>

	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE for TLS connection.</li> <li>• Start the TLS session and verify that TOE is able TOE is able to send audit logs to syslog server.</li> <li>• Verify the successful TLS connection via PCAP.</li> <li>• Verify with logs.</li> <li>• The evaluator physically interrupted the connection of that IT entity for a duration shorter than the application layer timeout but of sufficient length to interrupt the MAC layer.</li> <li>• Verify with the logs.</li> <li>• TLS Connection restore, once the cable plug it again without the TLS handshake.</li> <li>• Verify with the logs.</li> <li>• The evaluator start the TLS session again and physically interrupted the connection of that IT entity for a duration that exceeds the TOE's application layer timeout.</li> <li>• Verify the successful TLS connection via PCAP.</li> <li>• The evaluator physically interrupted the connection of that IT entity for a duration that exceeds the TOE's application layer timeout.</li> <li>• Verify with the logs.</li> <li>• TLS Connection restore, once the cable plug it again with the TLS handshake.</li> <li>• Verify with the logs.</li> <li>• • Verify with logs that the TLS handshake happen again.</li> </ul>
<b>Expected Test Results</b>	The TLSC connection should restore and encrypted once the physical connection will restore within the application layer timeout and also if it's exceeded the application layer time.
<b>Pass/Fail with Explanation</b>	Pass. In spite of physical disruption, the connection remains secure when connectivity is reestablished.

## FTP\_ITC.1/MACSEC Test #4

Item	Data
Test Assurance Activity	The evaluator shall evaluate this SFR in the manner specified in the NDcPP except that SNMPv3 and MACsec communications shall be tested in addition to any other selected protocols. Testing for these protocols is discussed in Section C.1.
Test Steps	<ul style="list-style-type: none"><li>• Start a normal MACsec connection between TOE and peer</li><li>• Verify the logs</li><li>• Physically interrupt the connection for 5 seconds and attempt to ping the peer. This will fail.</li><li>• Verify the logs</li><li>• When the connection is restored, the connection remains secure</li><li>• Verify the logs</li><li>• Physically interrupt the connection for over 6 seconds and attempt to ping the peer. This will fail.</li><li>• Verify the logs</li><li>• When the connection is restored again, the connection remains secure</li><li>• Verify the logs</li><li>•</li></ul>
Expected Test Results	Once the MACsec secure session is physically interrupted, TOE should not send plaintext traffic and the connection should restore once the interface is back to connected stage.
Pass/Fail with Explanation	Pass. The TOE does not send plaintext traffic when disconnected from the external entity. This meets the testing requirements.

### 15.1.2 Auth

## FCS\_CKM.2 RSA

Item	Data
Test Assurance Activity	Key Establishment Schemes



	The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1_5 by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses RSAES-PKCS1-v1_5.
<b>Pass/Fail with Explanation</b>	Pass. This testing was performed in conjunction with FCS_SSHS_EXT.1.2 Test #1, FCS_TLSC_EXT.1.1 Test #1, & FTP_ITC.1 Test #1.

## FCS\_CKM.2 FCC

Item	Data
<b>Test Assurance Activity</b>	<p><b>FCC Schemes using "safe-prime" groups</b></p> <p>The evaluator shall verify the correctness of the TSF's implementation of safe-prime groups by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses safe-prime groups. This test must be performed for each safe-prime group that each protocol uses.</p>
<b>Pass/Fail with Explanation</b>	Pass. This testing was performed in conjunction with FCS_SSHS_EXT.1.2 Test #1 & FTP_ITC.1 Test #4.

## FIA\_AFL.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>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):</p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Login into the TOE via SSH.</li> <li>• Set the TOE to lock out a user after five failed attempts.</li> </ul>

	<ul style="list-style-type: none"> <li>Starting login attempts with bad password.</li> <li>Checking that we can't login with good password. Verifying that user is locked.</li> <li>Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	The TOE should lock the user after the authentication attempts limit is reached and also authenticate attempts with valid credentials are no longer successful.
<b>Pass/Fail with Explanation</b>	Pass. The TOE did not allow authentication once the authentication attempt limit has been reached. This meets the testing requirements.

## FIA\_AFL.1 Test #2b

Item	Data
<b>Test Assurance Activity</b>	<p>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):</p> <p>Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows:</p> <p>If the <b>administrator action</b> 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).</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Login into the TOE via SSH.</li> <li>Set the TOE to lock out a user after five failed attempts &amp; lockout time period 5 min.</li> <li>Starting login attempts with bad password "asdfkjhqewrq".</li> <li>Now checked with good password and verify that the user is locked.</li> <li>Verify with the logs.</li> <li>Wait for more than 5 minutes that is lockout time period to successfully login into the TOE.</li> <li>Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	

	The TOE should locked the user after unsuccessful login attempts & it should unlock after few minutes.
<b>Pass/Fail with Explanation</b>	<b>Pass. TOE locked while unsuccessful attempts of login and user logged into the TOE after lockout time period which is 5 min.</b>

## FIA\_PMG\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configuring the password requirements.</li> <li>• Attempt to create good password that is "QWEyuiop()12345". (15-character password, the combination of 3 upper, 5 lower, 5 numeric and 2 special characters)</li> <li>• Show that the new user is created.</li> <li>• Attempt to create a good password that is "ASDGHjklz@#%789". (15-character password, the combination of 5 upper, 4 lower, 3 numeric and 3 special characters)</li> <li>• Show that the new user is created.</li> <li>• Attempt to create good password that is "LZXblk&amp;^%\$#9359". (15-character password, the combination of 3 upper, 3 lower, 4 numeric and 5 special characters)</li> <li>• Show that the new user is created.</li> <li>• Attempt to create a good password that is "HJTpoi\$!*\$!&amp;670". (15-character password, the combination of 3 upper, 3 lower, 3 numeric and 6 special characters)</li> <li>• Show that the new user is created.</li> <li>• Attempt to create good password that is "VBNMfghj)&amp;%5437". (15-character password, combination of 4 upper, 4 lower, 4 numeric and 3 special characters)</li> <li>• Show that the new user is created.</li> </ul>

<b>Expected Test Results</b>	The TOE should support the possible compositions of passwords, the evaluator shall ensure that all characters, and a minimum length listed in the requirement are supported.
<b>Pass/Fail with Explanation</b>	Pass. The TOE was able to create users with good combination of passwords. This meets the testing requirements.

## FIA\_PMG\_EXT.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the minimum length of the password.</li> <li>• Attempt to create a bad password that is "QWeyuiop()12345". (15-characters, combination of 2 upper, 6 lower, 5 numeric &amp; 2 special characters)</li> <li>• Verify that the user is not created.</li> <li>• Attempt to create a bad password "ASDGHJKlz@#%789". (9-characters, combination of 7 upper, 2 lower characters, 3 numeric &amp; 3 special characters)</li> <li>• Verify that the user is not created.</li> <li>• Attempt to create bad password "LZXOpblk&amp;^%\$#93". (15-characters, combination of 4 upper, 4 lower, 2 numeric characters &amp; 5 special characters)</li> <li>• Verify that the user is not created.</li> <li>• Attempt to create bad password "HJTGHpoilk67098". (15-characters, 5 upper, 5 lower &amp; 5 numeric characters)</li> <li>• Verify that the user is not created.</li> </ul>
<b>Expected Test Results</b>	The TOE should not create new users with password which does not meet the requirements.
<b>Pass/Fail with Explanation</b>	Pass. The TOE was not able to create users with bad passwords. This meets the testing requirements.

## FIA\_UIA\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>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:</p> <p>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&amp;A information results in the ability to access the system, while providing incorrect information results in denial of access.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Log onto the TOE local connection with incorrect credentials &amp; make sure that banner is present prior to login.</li> <li>• Verify the failure attempt via logs.</li> <li>• Log onto the TOE via local connection using correct credentials and make sure that banner is present prior to login.</li> <li>• Verify the successful attempts via logs.</li> <li>• Log onto the TOE remotely via SSH CLI with incorrect credentials &amp; make sure that banner is present prior to login.</li> <li>• Verify the failure attempt via logs.</li> <li>• Log onto the TOE remotely via SSH CLI with correct credentials &amp; also make sure that banner is present prior to login.</li> <li>• Verify the successful attempts via logs.</li> </ul>
<b>Expected Test Results</b>	<p>The access to the TOE via local connection require correct credential else access will deny.</p>
<b>Pass/Fail with Explanation</b>	<p>Pass. Providing incorrect credentials results denied to access the TOE and providing correct credentials results in access allowed to the TOE. This meets the testing requirements.</p>

## FIA\_UIA\_EXT.1 Test #2

Item	Data

<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts to access the TOE with an unauthorized user as config and it will fail.</li> <li>• Verify that banner is displayed prior to login.</li> <li>• Verify failure login attempt via logs.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject the services to unauthorized user while establishing SSH session.
<b>Pass/Fail with Explanation</b>	Pass. No system services are available to an unauthenticated user connecting remotely. This meets the testing requirements.

### FIA\_UIA\_EXT.1 Test #3

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The evaluator attempts to access the TOE with an unauthorized user as config and it will fail.</li> <li>• Verify that banner is displayed prior to login.</li> <li>• Verify with the failure logs.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject the services to unauthorized user while establishing local connection.
<b>Pass/Fail with Explanation</b>	Pass. No system services are available to an unauthenticated user connecting locally. This meets the testing requirements.

## FIA\_UAU.7 Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	TOE should display the authentication information obscured feedback while login through console.
<b>Expected Test Results</b>	Verify with logs at most obscured feedback is provided while entering the authentication information
<b>Pass/Fail with Explanation</b>	Pass. At the directly connected login prompt, the TOE does not provide anything more than obscured feedback. This meets the testing requirements.

## FMT\_MOF.1/ManualUpdate Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• Create an unprivileged user on the TOE.</li><li>• Login into the TOE with unprivileged user.</li><li>• Attempt to perform manual updates on the TOE, this will fail.</li><li>• Verify with the logs.</li></ul>
<b>Expected Test Results</b>	Unprivileged user of the TOE are not able to perform a software update on the it.
<b>Pass/Fail with Explanation</b>	

Pass. Unprivileged user of the TOE are not able to perform a software update on it. These meets the testing requirements.

## FMT\_MOF.1/ManualUpdate Test #2

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Pass/Fail with Explanation</b>	This test case is covered by the test for FPT_TUD_EXT.1.1 Test #1.

## FMT\_MOF.1/Services Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) without prior authentication as Security Administrator (either by authenticating as a user with no administrator privileges, if possible, or without prior authentication at all). The attempt to enable/disable this service/these services 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 enable/disable this service/these services 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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create an unprivileged user on the TOE.</li> <li>• Login into the TOE with unprivileged user.</li> <li>• Attempt to modify the service of the TOE with unprivileged user.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	The TOE's user without prior authentication cannot perform actions.



<b>Pass/Fail with Explanation</b>	Pass. User without prior authentication/privilege was unable to perform actions on the TOE.
-----------------------------------	---

## FMT\_MOF.1/Services Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) with prior authentication as Security Administrator. The attempt to enable/disable this service/these services should be successful.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a privileged user on the TOE.</li> <li>• Login into the TOE via privileged user.</li> <li>• Attempt to modify the service on the TOE with privileged user.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	The TOE's user with prior authentication/privilege was able to perform actions on the TOE.
<b>Pass/Fail with Explanation</b>	Pass. User with prior authentication/privilege was able to modify service parameter on the TOE.

## FMT\_MTD.1/CryptoKeys Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create an unprivileged user.</li> <li>• Login into the TOE with unprivileged user.</li> <li>• Attempt to modify the crypto keys with unprivileged user.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	TOE's unauthorized user cannot perform security related configurations on it.
<b>Pass/Fail with Explanation</b>	Pass. Unprivileged user cannot perform security related configurations on the TOE. This meets the testing requirements.

## FMT\_MTD.1/CryptoKeys Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a privileged user on the TOE.</li> <li>• Login into the TOE with privilege user.</li> <li>• Attempt to modify the crypto keys with privilege user.</li> <li>• Verify with the logs</li> </ul>
<b>Expected Test Results</b>	TOE's authenticated user can perform security related configurations on it.
<b>Pass/Fail with Explanation</b>	Pass. Authenticated user can perform security related configurations on the TOE. This meets the testing requirements.

### FMT\_SMF.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Pass/Fail with Explanation</b>	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.

### FMT\_SMR.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Pass/Fail with Explanation</b>	Pass. There are two interfaces where these can be tested (over the remote SSH and local console). The evaluator has met this requirement through execution of the entirety of this test report by performing actions via both TOE interfaces.

### FTA\_SSL.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
	<ul style="list-style-type: none"><li>• Login into the TOE &amp; Set remote timeout period to 60 seconds &amp; logout from the TOE.</li></ul>

<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Login into the TOE via SSH &amp; show clock.</li> <li>• Wait for 62 seconds &amp; Verify the session is terminated.</li> <li>• Verify with the logs.</li> <li>• Login into the TOE &amp; Set remote timeout period to 120 seconds &amp; logout from the TOE.</li> <li>• Login into the TOE via SSH &amp; show clock.</li> <li>• Wait for 122 seconds &amp; Verify the session is terminated.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	The remote administrative time out periods can be set by the administrative user and the TOE should enforce the configured inactivity period in each instance.
<b>Pass/Fail with Explanation</b>	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.

## FTA\_SSL.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Login into the TOE via console and terminate the console session .</li> <li>• Verify that the console session is terminated.</li> </ul>
<b>Expected Test Results</b>	The TOE allows user to terminate the local connected administrative sessions with exit or log off.
<b>Pass/Fail with Explanation</b>	Pass. The TOE allows user to terminate the directly connected administrative sessions. This meets the testing requirements.

## FTA\_SSL.4 Test #2

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• Log onto the TOE via SSH &amp; terminate the session.</li><li>• Verify that the SSH session is closed.</li></ul>
<b>Expected Test Results</b>	The TOE allows user to terminate the remotely connected administrative sessions with exit or log off.
<b>Pass/Fail with Explanation</b>	Pass. The TOE allows user to terminate the remote administrative sessions. This meets the testing requirements.

## FTA\_SSL\_EXT.1.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• Login into the TOE &amp; Set remote timeout period to 60 seconds &amp; logout from the TOE.</li><li>• Login into the TOE via console &amp; show clock.</li><li>• Wait for 62 seconds &amp; verify the session is terminated.</li><li>• Verify with the logs.</li><li>• Login into the TOE &amp; Set remote timeout period to 120 seconds &amp; logout from the TOE.</li><li>• Login into the TOE via console &amp; show clock.</li><li>• Wait for 122 seconds &amp; Verify the session is terminated.</li><li>• Verify with the logs.</li></ul>

<b>Expected Test Results</b>	The local administrative logged out time-period can be able to be set to multiple values and in each instance, the TOE should logged out the user after the configured time-period.
<b>Pass/Fail with Explanation</b>	Pass. The local administrative inactive time period was able to be set to multiple values. In each instance, the TOE logged the user out after the configured time. This meets the testing requirements

### FTA\_TAB.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure access banners on TOE.</li> <li>• Verify with the logs.</li> <li>• Log into the TOE via SSH and verify that the configured banner is present.</li> <li>• Log into the TOE via console and verify that the configured banner is present.</li> </ul>
<b>Expected Test Results</b>	A configured access banner should display while login into the TOE via locally and remotely.
<b>Pass/Fail with Explanation</b>	Pass. An access banner can be set for all the methods that can be used to access the device. This meets the testing requirements.

### FTP\_TRP.1/Admin Test #1

Item	Data
------	------

<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Login into the TOE via SSH.</li> <li>• Verify with the pcap captured.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	While logging into the TOE remotely user should successfully access the device.
<b>Pass/Fail with Explanation</b>	Pass. The user established the successful connection with the TOE remotely.

## FTP\_TRP.1/Admin Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Login into the TOE via SSH.</li> <li>• Verify with the pcap captured.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	For each type of communication channel with the TOE, the channel data should not in plaintext.
<b>Pass/Fail with Explanation</b>	Pass. Remote administrative access to the TOE is over secure protected channels and the data was not sent in plaintext. This meets the testing requirements.

## 15.1.3 SSHS

### FCS\_SSHS\_EXT.1.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: For each supported client public-key authentication algorithm, the evaluator shall configure a remote client to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH client to demonstrate the use of all applicable public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test.</p> <p><b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• Generate a new RSA key</li><li>• Convert the .pub file into base64 encoding file</li><li>• Copy the file onto the TOE</li><li>• Configure the user to use public key while authentication</li><li>• Log into the TOE SSH with RSA-based authentication</li><li>• Verify the logs<ul style="list-style-type: none"><li>• Verify the pcap</li></ul></li></ul>
<b>Expected Test Results</b>	Verify with logs and pcap to login into the TOE via SSH session using RSA key
<b>Pass/Fail with Explanation</b>	Pass. The TOE supports each of the claimed public key algorithms. This meets the testing requirements



## FCS\_SSHS\_EXT.1.2 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2: The evaluator shall choose one client public key authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails.</p> <p><b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Generate new public-private RSA key pair on the VM</li> <li>• Attempt the login without importing new public key onto the TOE</li> <li>• Verify that the connection via packet capture</li> <li>• Verify the logs</li> </ul> <p>Verify with pcap.</p>
<b>Expected Test Results</b>	Login into the TOE via SSH session using new RSA key without importing into TOE should fail.
<b>Pass/Fail with Explanation</b>	Pass. The TOE does not allow public key authentication if the public key of the SSH user have not uploaded to the TOE. This meets the test requirements.

## FCS\_SSHS\_EXT.1.2 Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>Test 3: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication succeeds when the correct password is provided by the connecting SSH client.</p> <p><b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Ensure the TOE supports password-based authentication</li> <li>• Ensure the TOE supports password-based authentication</li> </ul>

	<ul style="list-style-type: none"> <li>• Log into the TOE via SSH with password authentication</li> <li>• Verify authentication logs</li> <li>• Verify with pcap capture that SSH session was established</li> </ul>
<b>Expected Test Results</b>	TOE should support the public-key authentication algorithm when remote client establishing SSH connection.
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to establish a connection with a remote SSH user when correct authentication credentials are presented. This meets the testing requirements.

### FCS\_SSHS\_EXT.1.2 Test #4

Item	Data
<b>Test Assurance Activity</b>	<p>Test 4: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication fails when the incorrect password is provided by the connecting SSH client.</p> <p><b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Ensure the TOE supports password-based authentication.</li> <li>• Attempt to Log into the TOE via SSH with correct username incorrect password-based authentication parameters (will fail).</li> <li>• Verify with authentication logs reflect failures.</li> </ul>
<b>Expected Test Results</b>	Toe should not accept the password-based authentication while providing incorrect password by the user
<b>Pass/Fail with Explanation</b>	Pass. The TOE is not able to establish a connection with a remote SSH user when incorrect authentication credentials are presented. This meets the testing requirements.

### FCS\_SSHS\_EXT.1.3 Test #1

Item	Data
------	------

<b>Test Assurance Activity</b>	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use SSHS acumen tool to send bad length packet.</li> <li>• Verify with the logs.</li> <li>• Verify with the pcap.</li> </ul>
<b>Expected Test Results</b>	TOE receives a packet larger than specified will dropped that packet.
<b>Pass/Fail with Explanation</b>	Pass. The TOE drops large packets that are received within an SSH session. This meets the testing requirements.

### FCS\_SSHS\_EXT.1.4 Test #1

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	<p>The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection.</p> <p>To verify this, the evaluator shall start session establishment for an SSH connection from a remote client (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS. The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test.</p> <p>If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE to support AES-128 for encryption algorithm. (claimed cipher).</li> <li>• Establish an SSH session from remote client to the TOE ciphers defined in the TSS.</li> <li>• Verify that the SSH session was encrypted using AES128-ctr via logs.</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify that the SSH session was encrypted using AES128-ctr via pcap.</li> <li>• Configure the TOE to support AES-256 for encryption algorithm (claimed cipher).</li> <li>• Establish an SSH session from remote client to the TOE with the ciphers defined in the TSS.</li> <li>• Verify that the SSH session was encrypted using AES256-ctr via logs.</li> <li>• Verify that the SSH session was encrypted using AES256-ctr via pcap.</li> </ul>
<b>Expected Test Results</b>	The TOE should support only claimed ciphers and cryptographic primitives while establishing an SSH.
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to make SSH connections with each claimed algorithm. This meets the testing requirements.

### FCS\_SSHS\_EXT.1.5 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.</p> <p><b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Generate an ssh-rsa host key pair on the TOE.</li> <li>• Login to the TOE using the host public key and verify that the session is established.</li> <li>• Verify via logs that the session was established.</li> </ul> <p>Verify via packet capture that the configured host key algorithm was used.</p>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• TOE logs shows successful establishment of the SSH connection.</li> <li>• Packet capture shows session establishment with the configured host key algorithm.</li> </ul>

<b>Pass/Fail with Explanation</b>	Pass. The remote client is able to establish a successful SSH connection using each one of the claimed host public key algorithms.
-----------------------------------	--

## FCS\_SSHS\_EXT.1.5 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected.</p> <p><b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE to reject SSH sessions using the unsupported ssh-dss algorithm.</li> <li>• Attempt to establish an SSH session using the ssh-dss host public key algorithm.</li> <li>• Verify that the connection is refused via packet capture.</li> <li>• Verify that the SSH session was refused using ssh-dss via log.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• TOE logs verify connection establishment using an unsupported public key algorithm(ssh-dss) is denied by TOE.</li> <li>• Packet Capture verifies connection establishment using an unsupported public key algorithm(ssh-dss) is denied by TOE.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The remote client rejects the SSH connection using each non claimed host public key algorithms.

## FCS\_SSHS\_EXT.1.6 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: [conditional, if an <b>HMAC or AEAD_AES_*_GCM</b> algorithm is selected in the ST] The evaluator shall establish an SSH connection using each of the algorithms, except “implicit”, specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.</p>

	Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The TOE support <b>HMAC-SHA-1</b> for the message integrity algorithm.</li> <li>• Establish an SSH session with the configured supported algorithms.</li> <li>• Verify via logs that the algorithm was used.</li> <li>• Verify with the pcap.</li> <li>• The TOE support <b>HMAC-SHA2-256</b> for the message integrity algorithm.</li> <li>• Establish an SSH session with the configured supported algorithms.</li> <li>• Verify via logs that the algorithm was used.</li> <li>• Verify with the pcap.</li> <li>• The TOE support <b>HMAC-SHA2-512</b> for the message integrity algorithm.</li> <li>• Establish an SSH session with the configured supported algorithms.</li> <li>• Verify via logs that the algorithm was used.</li> <li>• Verify with the pcap.</li> </ul>
<b>Expected Test Results</b>	The TOE should support message integrity algorithms while establishing SSH connection.
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to make SSH connections with each claimed data integrity algorithm. This meets the testing requirements.

## FCS\_SSHS\_EXT.1.6 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: [conditional, if an <b>HMAC or AEAD_AES_*_GCM</b> algorithm is selected in the ST] The evaluator shall configure an SSH client to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the SSH client to the TOE and

	<p>observe that the attempt fails.</p> <p>Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Attempt to establish an SSH session using unsupported mac.</li> <li>• Verify the logs of invalid traffic.</li> <li>• Verify Wireshark does not continue negotiation.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject unsupported mac algorithm while establishing SSH connection.
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects SSH connections using the unsupported MAC for data integrity. This meets the testing requirements.

### FCS\_SSHS\_EXT.1.7 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Attempt to establish an SSH session using diffiehellman-group1-sha1.</li> <li>• Capture the traffic between the devices.</li> <li>• Verify with pcap that the session was not established.</li> </ul>

<b>Expected Test Results</b>	TOE should not support diffiehellman-group1-sha1 algorithm while establishing SSH session.
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects SSH connections using diffiehellman-group1-sha1 (a non-approved algorithm) for key exchange. This meets the testing requirements.

## FCS\_SSHS\_EXT.1.7 Test #2

Item	Data
<b>Test Assurance Activity</b>	For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Establish an SSH session with the configured diffie-hellman-group14-sha1 key algorithms.</li> <li>Capture the traffic between the devices.</li> <li>Verify that the session was established.</li> </ul>
<b>Expected Test Results</b>	The TOE should support diffie-hellman-group14-sha1 key algorithms while establishing SSH session.
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to make SSH connections with each claimed data key exchange method. This meets the testing requirements.

## FCS\_SSHS\_EXT.1.8 Test #1t

Item	Data
------	------



<b>Test Assurance Activity</b>	<p>The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the <b>time-based threshold</b> and the traffic-based threshold.</p> <p>For testing of the time-based threshold, the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).</p> <p>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.</p> <p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configuring the TOE with SSH REKEY.</li> <li>• Establish SSH session with the TOE and keep it idle for 30 minutes.</li> <li>• Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<p>The Toe should negotiate the rekey after 30 minutes</p>
<b>Pass/Fail with Explanation</b>	<p>Pass. The TOE initiates a rekey every 30 mins. This meets the testing requirements.</p>

### FCS\_SSHS\_EXT.1.8 Test #1b

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the <b>traffic-based</b> threshold.</p>

	<p>For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH client and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHS_EXT.1.8).</p> <p>The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).</p> <p>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.</p> <p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).</p> <p>In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met:</p> <ol style="list-style-type: none"> <li>1. An argument is present in the TSS section describing this hardware- based limitation and</li> <li>2. All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified.</li> </ol>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE for volume rekey.</li> <li>• Establish an SSH session with the TOE and transfer the file of 1100 MB on the TOE.</li> <li>• Verify via logs.</li> </ul>

<b>Expected Test Results</b>	The Toe should negotiate the rekey after transferring more than one GB data
<b>Pass/Fail with Explanation</b>	Pass. The TOE initiates a rekey after 1024 MB data traffic. This meets the testing requirements.

## 15.1.4 TLSC

### FCS\_TLSC\_EXT.1.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	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 which ciphersuite is being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE for TLS connection.</li> <li>• Create Root CA &amp; ICA Trustpoint on the TOE.</li> <li>• Authenticate to the CA &amp; ICA.</li> <li>• Configure the server certificate.</li> <li>• Start the TLS connection with supported cipher TLS_RSA_WITH_AES128_SHA &amp; version TLS_1.2.</li> <li>• Verify with the logs.</li> <li>• Verify with the PCAP.</li> <li>• Start the TLS connection with supported cipher TLS_RSA_WITH_AES256_SHA &amp; version TLS_1.2.</li> <li>• Verify with the logs.</li> <li>• Verify with the PCAP.</li> </ul>
<b>Expected Test Results</b>	TLS connection should establish using each of the claimed ciphersuites.
<b>Pass/Fail with Explanation</b>	Partially Pass. The TOE connects to a remote TLS server using the claimed ciphersuites with TLSv1.2. This meets the testing requirements.

## FCS\_TLSC\_EXT.1.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	<ol style="list-style-type: none"> <li>1. 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.</li> </ol>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE for TLS connection.</li> <li>• Create a server certificate with the Server Authentication in the extendedKeyUsage field.</li> <li>• Attempt to establish the TLS connection.</li> <li>• Verify with the logs.</li> <li>• Verify with the PCAP.</li> <li>• Remove server authentication EKU from server certificate.</li> <li>• Attempt TLS connection which should fail.</li> <li>• Verify the failure connection via pcap.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	The TOE should reject a connection to a server using an invalid server certificate.
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects a connection to a server using an invalid server certificate. This meets the testing requirements.

## FCS\_TLSC\_EXT.1.1 Test #3

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall send a server certificate in the TLS connection that does not match the server-selected ciphersuite (for example, send an 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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer FCS_TLSC_EXT.1.1 Test #1 for TLS configurations on the TOE.</li> <li>• Configure the server certificate.</li> <li>• Attempt to make a connection with the TOE.</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify the connection is refused via packet capture.</li> <li>• Verify the connection is refused via logs.</li> </ul>
<b>Expected Test Results</b>	The TOE denied a connection to a server using a certificate that doesn't match the Ciphersuite.
<b>Pass/Fail with Explanation</b>	Pass. The TOE denied a connection to a server using a certificate that doesn't match the ciphersuite. This meets the testing requirements.

### FCS\_TLSC\_EXT.1.1 Test #4a

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer FCS_TLSC_EXT.1.1 Test #1 for TLS configurations on the TOE.</li> <li>• The AcumenTLS tool is run and attempt to make a connection with the TOE.</li> <li>• Verify the connection is refused via packet capture.</li> <li>• Verify the connection is refused via logs.</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the TOE denied the connection to a server using a NULL ciphersuite
<b>Pass/Fail with Explanation</b>	Pass. The TOE denied the connection to a server using a NULL ciphersuite. This meets the testing requirements.

### FCS\_TLSC\_EXT.1.1 Test #4b

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer FCS_TLSC_EXT.1.1 Test #1 for TLS configurations on the TOE.</li> <li>• The AcumenTLS tool is run and attempt to make a connection with the TOE.</li> <li>• Verify the connection is refused via packet capture.</li> <li>• Verify the connection is refused via logs.</li> </ul>

<b>Expected Test Results</b>	Verify with logs that the TOE denied the connection when server's selected cipher suite is modified.
<b>Pass/Fail with Explanation</b>	Pass. The TOE denied the connection when server's selected cipher suite is modified. This meets the testing requirements.

### **FCS\_TLSC\_EXT.1.1 Test #5a**

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer FCS_TLSC_EXT.1.1 Test #1 for TLS configurations on the TOE.</li> <li>• The AcumenTLS tool is run and attempt to make a connection with the TOE.</li> <li>• Verify the connection is refused via packet capture.</li> <li>• Verify the connection is refused via logs.</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the TOE should denied the connection when server hello sends unsupported TLS version.
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects the connection after key Exchange when server's selected unsupported TLS version. This does not meets the testing requirements.

### **FCS\_TLSC\_EXT.1.1 Test #6a**

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	Modify a byte in the Server Finished handshake message and verify that the handshake does not finish successfully and no application data flows.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer FCS_TLSC_EXT.1.1 Test #1 for TLS configurations on the TOE.</li> <li>• Attempt to make a connection with the TOE.</li> <li>• Verify the connection is refused via packet capture.</li> <li>• Verify the connection is refused via logs.</li> </ul>
<b>Expected Test Results</b>	Verify with logs when byte in the Server Finished handshake message is modified, the TOE should not complete the connection.

<b>Pass/Fail with Explanation</b>	Pass. When a byte in the Server Finished handshake message is modified, the TOE does not complete the connection. This meets the test requirements.
-----------------------------------	---

### FCS\_TLSC\_EXT.1.1 Test #6b

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer FCS_TLSC_EXT.1.1 Test #1 for TLS configurations on the TOE.</li> <li>• The AcumenTLS tool is run and attempt to make a connection with the TOE.</li> <li>• Verify the connection is refused via packet capture.</li> <li>• Verify the connection is refused via logs.</li> </ul>
<b>Expected Test Results</b>	Verify with logs that Connection should be rejected when garbled message is sent.
<b>Pass/Fail with Explanation</b>	Pass. Connection was rejected when garbled message was sent.

### FCS\_TLSC\_EXT.1.1 Test #6c

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Note</b>	<i>TLS Tool: AcumenTLS (NIAP provided tool (<a href="https://github.com/commoncriteria/tls-cc-tools">https://github.com/commoncriteria/tls-cc-tools</a>) updated for usability)</i>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE for TLS connection</li> <li>• Create Root CA &amp; ICA Trustpoint on the TOE</li> <li>• Authenticate to the CA &amp; ICA</li> <li>• Configure the server certificate</li> </ul>

	<ul style="list-style-type: none"> <li>• The AcumenTLS tool is run and attempt to make a connection with the TOE</li> <li>• Verify the connection is refused via packet capture</li> <li>• Verify the connection is refused via logs</li> </ul>
<b>Expected Test Results</b>	The modified TLS connection should be rejected.
<b>Pass/Fail with Explanation</b>	Pass. The modified TLS connection was rejected. This meets the testing requirements.

### FCS\_TLSC\_EXT.1.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>This test is applicable if <b>TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.</b></p> <p>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.</p> <p>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.</p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the CA and ICA certificates on the TOE as shown in the FCS_TLSC_EXT.1.1 Test #1.</li> <li>• TOE's settings and server certificate details.</li> </ul>



	<ul style="list-style-type: none"> <li>• The evaluator attempted to connect to a server using a certificate missing the SAN but with a CN that does not meet the reference identifier.</li> <li>• Verify the connection is refused via packet capture.</li> <li>• Verify the connection is refused via logs.</li> </ul>
<b>Expected Test Results</b>	A connection should not established when presented a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier.
<b>Pass/Fail with Explanation</b>	Pass. A connection was not established when presented a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. This meets the testing requirements.

## FCS\_TLSC\_EXT.1.2 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>This test is applicable if <b>TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.</b></p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the CA and ICA certificates on the TOE as shown in the FCS_TLSC_EXT.1.1 Test #1.</li> <li>• TOE's settings and server certificate details.</li> <li>• The evaluator attempted to connect to a server using a certificate contains CN matches reference identifier &amp; incorrect SAN which does not match the reference identifier. The connection should fail.</li> <li>• Verify the connection is refused via packet capture.</li> <li>• Verify the connection is refused via logs.</li> </ul>

<b>Expected Test Results</b>	A connection should not established when presented 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.
<b>Pass/Fail with Explanation</b>	Pass. A connection was not established when presented 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. This meets the testing requirements.

### FCS\_TLSC\_EXT.1.2 Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>This test is applicable if <b>TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.</b></p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the CA and ICA certificates on the TOE as shown in the FCS_TLSC_EXT.1.1 Test #1.</li> <li>• TOE's settings and server certificate details.</li> <li>• The evaluator attempted to connect to a server using a certificate contains CN matches reference identifier &amp; does not contain SAN, The connection will pass.</li> <li>• Verify the connection is successful via packet capture.</li> <li>• Verify the connection is successful via logs.</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the Connection was successful when presented certificate has only CN matches to reference identifier
<b>Pass/Fail with Explanation</b>	Pass. Connection was successful when presented certificate has only CN matches to reference identifier. This meets the requirement.

## FCS\_TLSC\_EXT.1.2 Test #4

Item	Data
Test Assurance Activity	<p>This test is applicable if <b>TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.</b></p> <p>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).</p>
Test Steps	<ul style="list-style-type: none"><li>• Configure the CA and ICA certificates on the TOE as shown in the FCS_TLSC_EXT.1.1 Test #1.</li><li>• TOE's settings and server certificate details.</li><li>• The evaluator attempted to connect to a server using a certificate with correct SAN &amp; incorrect CN. The connection will pass.</li><li>• Verify the connection via packet capture.</li><li>• Verify with the logs.</li></ul>
Expected Test Results	Verify with a connection that should established when presented server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches.
Pass/Fail with Explanation	Pass. A connection was established when presented server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. This meets the testing requirements.

## FCS\_TLSC\_EXT.1.2 Test #5 (1)

Item	Data
Test Assurance Activity	This test is applicable if <b>TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.</b>

	<p>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):</p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the CA and ICA certificates on the TOE as shown in the FCS_TLSC_EXT.1.1 Test #1.</li> <li>• TOE's settings and server certificate details.</li> <li>• The evaluator attempted to connect a server using a certificate that contains a wildcard that is not in the left-most label of the reference identifier.</li> <li>• Verify the failure connection via packet capture.</li> <li>• Verify the failure connection via logs.</li> </ul>
<b>Expected Test Results</b>	Verify with logs when a server certificate contains a wildcard that is not in the left-most label of the presented identifiers), the TOE the client rejects the connection.
<b>Pass/Fail with Explanation</b>	Pass. When a server certificate contains a wildcard that is not in the left-most label of the presented identifiers, the TOE the client rejects the connection. This meets the testing requirements.

### FCS\_TLSC\_EXT.1.2 Test #5 (2)(a)

Item	Data
<b>Test Assurance Activity</b>	<p>This test is applicable if <b>TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.</b></p> <p>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):</p> <p>The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com).</p>

	<p>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.</p> <p>(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.)</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the CA and ICA certificates on the TOE as shown in the FCS_TLSC_EXT.1.1 Test #1.</li> <li>• TOE's settings and server certificate details.</li> <li>• The evaluator attempted to connect a server using a certificate that contains a wildcard that is not in the left-most label of the reference identifier.</li> <li>• Verify the connection via packet capture.</li> <li>• Verify the connection via logs.</li> </ul>
<b>Expected Test Results</b>	The TOE should support wildcard type reference identifier.
<b>Pass/Fail with Explanation</b>	Pass. TOE support wildcard type reference identifier.

### FCS\_TLSC\_EXT.1.2 Test #5 (2)(b)

Item	Data
<b>Test Assurance Activity</b>	<p>This test is applicable if <b>TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.</b></p> <p>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):</p> <p>The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com).</p>

	<p>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.</p> <p>(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.)</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the CA and ICA certificates on the TOE as shown in the FCS_TLSC_EXT.1.1 Test #1.</li> <li>• TOE's settings and server certificate details.</li> <li>• The evaluator attempted to connect a server using a certificate that contains a wildcard that is not in the left-most label of the reference identifier. The connection fails.</li> <li>• Verify the connection is refused via packet capture.</li> <li>• Verify the connection is refused via logs.</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the server only makes connections based on valid presented certificate.
<b>Pass/Fail with Explanation</b>	Pass. The server only makes connections based on valid presented certificate. This meets the testing requirements.

### FCS\_TLSC\_EXT.1.2 Test #5 (2)(c)

Item	Data
<b>Test Assurance Activity</b>	<p>This test is applicable if <b>TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.</b></p> <p>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):</p> <p>The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com).</p>

	<p>The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails.</p> <p>(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.)</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the CA and ICA certificates on the TOE as shown in the FCS_TLSC_EXT.1.1 Test #1.</li> <li>• TOE's settings and server certificate details.</li> <li>• The evaluator attempted to connect a server using a certificate that contains a wildcard that is not in the left-most label of the reference identifier. The connection fails.</li> <li>• Verify the connection is refused via packet capture.</li> <li>• Verify the connection is refused via logs.</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the server only makes connections based on valid presented certificate.
<b>Pass/Fail with Explanation</b>	Pass. The server only makes connections based on valid presented certificate. This meets the testing requirements.

### FCS\_TLSC\_EXT.1.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Pass/Fail with Explanation</b>	Test covered by FIA_X509_EXT.1.1/Rev Test #1. When a complete certificate trust chain is present, the TOE is able to make a successful connection. When an incomplete certificate trust chain is present, the TOE is not able to make a successful connection. This meets the testing requirements.

### FCS\_TLSC\_EXT.1.3 Test #2

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted.</p> <p>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).</p> <p>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.</p>
<b>Pass/Fail with Explanation</b>	<p>Test covered by FCS_TLSC_EXT.1.1 Test #1, FIA_X509_EXT.1.1/Rev Test #1(TLS), FIA_X509_EXT.1.1/Rev Test #2 and FIA_X509_EXT.1.1/Rev Test #3. When a complete certificate trust chain is present, the TOE is able to make a successful connection. When an incomplete certificate trust chain is present, the TOE is not able to make a successful connection.</p>

### FCS\_TLSC\_EXT.1.3 Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>The purpose of this test to verify that only selected certificate validation failures could be administratively overridden. <b>If any override mechanism is defined for failed certificate validation</b>, 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 extendedKeyUsage field) but is otherwise valid and signed by a trusted CA.</p> <p>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.</p>
<b>Pass/Fail with Explanation</b>	<p>Test covered by FIA_X509_EXT.1.1/Rev Test #1b and FIA_X509_EXT.1.2/Rev Test #2. There is no override mechanism provided to the Administrator. When a complete certificate trust chain is present, the TOE is able to make a successful connection. When an incomplete certificate that does not contain a valid entry in one of the mandatory fields or parameters is presented, the TOE is not able to make a successful connection. This meets the testing requirements.</p>



## 15.1.4 Update

### FPT\_TST\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>It is expected that at least the following tests are performed:</p> <ul style="list-style-type: none"> <li>a) Verification of the integrity of the firmware and executable software of the TOE</li> <li>b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs.</li> </ul> <p>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.</p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Log into the console and reload the device.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	<p>Verify the integrity of the firmware and executable software of the TOE with logs.</p> <p>Also verify the correct operation of the cryptographic functions with logs.</p>
<b>Pass/Fail with Explanation</b>	<p>Pass. The TSS of the ST states that, FIPS POST includes cryptographic modules and software integration tests. Validator found that FIPS POST test has passed. These meets the requirement.</p>

### FPT\_TUD\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator performs the version verification activity to determine the current version of the product. If a trusted update can be installed on the TOE with a delayed activation, the evaluator shall also query the most recently installed version (for this test the TOE shall be in a state where these two versions match). The evaluator obtains a legitimate update using procedures</p>

	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Show current version of software.</li> <li>• Upload new software onto TOE.</li> <li>• Install the packages onto the TOE.</li> <li>• Activate the added packages and reload the device.</li> <li>• Verify the version of the TOE.</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the TOE software should be able to be updated with an image that passes the integrity test is used
<b>Pass/Fail with Explanation</b>	Pass. The TOE software was able to be updated when an image that passes the integrity test is used. This meets the testing requirements.

## FPT\_TUD\_EXT.1 Test #2 (a)

Item	Data
<b>Test Assurance Activity</b>	<p>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).</p> <p>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:</p> <p>1) A modified version (e.g. using a hex editor) of a legitimately signed update</p>

	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Confirm the version of the TOE.</li> <li>• Show the correct image signature on Hex Editor.</li> <li>• Show the Bad_sign(corrupted) image signature on Hex Editor.</li> <li>• Copy new corrupted image.</li> <li>• Attempt to update the TOE software using the corrupt image.</li> <li>• Verify the version of the TOE again just to make sure that it is still same and not updated.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the TOE actively rejects software update that are corrupt.
<b>Pass/Fail with Explanation</b>	Pass. The TOE actively rejects software updates that are corrupt. This meets the testing requirements.

### FPT\_TUD\_EXT.1 Test #2 (b)

Item	Data
<b>Test Assurance Activity</b>	[conditional]: If <b>the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE</b> the following test shall be performed (otherwise the test shall be omitted).

	<p>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:</p> <p>2) An image that has not been signed</p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Confirm the version of the TOE.</li> <li>• Show the correct image signature on Hex Editor.</li> <li>• Show the No_sign(corrupted) image signature on Hex Editor.</li> <li>• Copy new corrupted image.</li> <li>• Attempt to update the TOE software using the image which not signed.</li> <li>• Verify the version of the TOE again just to make sure that it is still same and not updated.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the TOE software was able to detect when an image was not signed and rejected the image
<b>Pass/Fail with Explanation</b>	Pass. The TOE software was able to detect when an image was not signed and rejected the image. This meets the testing requirements.

## FPT\_TUD\_EXT.1 Test #2 (c)

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>[conditional]: If <b>the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE</b> the following test shall be performed (otherwise the test shall be omitted).</p> <p>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:</p> <p>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)</p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Confirm the version of the TOE.</li> <li>• Copy new corrupted image.</li> <li>• Attempt to update the TOE software using the image which has invalid signature.</li> <li>• Verify the version of the TOE again just to make sure that it is still same and not updated.</li> <li>• Verify with the logs.</li> </ul>
<b>Expected Test Results</b>	<p>Verify with logs that the TOE actively rejects software updates when an image signature is invalid.</p>
<b>Pass/Fail with Explanation</b>	<p>The TOE actively rejects software updates when an image signature is invalid. This meets the testing requirements.</p>

## 15.1.5 X509-Rev

### FIA\_X509\_EXT.1.1/Rev Test #1a

Item	Data
<b>Test Assurance Activity</b>	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).
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• Configure the TOE for TLS connection</li><li>• Create Root CA &amp; ICA trustpoint</li><li>• Authenticate to the CA &amp; ICA</li><li>• Create a signed server certificate with root CA</li><li>• Attempt to connect to the TOE with the full chain of proper certificates</li><li>• Verify the connection is established via packet capture</li><li>• Verify the connection is successful via log</li></ul>
<b>Expected Test Results</b>	Verify with logs that when complete certificate trust chain is present, the TOE is able to make a successful connection
<b>Pass/Fail with Explanation</b>	Pass. When a complete certificate trust chain is present, the TOE is able to make a successful connection. This meets the testing requirements.

### FIA\_X509\_EXT.1.1/Rev Test #1b

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• For TOE configurations, refer to FIA_X509_EXT.1.1 Test #1</li></ul>

	<ul style="list-style-type: none"> <li>• Delete the root certificate from the chain</li> <li>• Attempt to connect to the TOE without the Root-CA2</li> <li>• Verify that the connection failed via packet capture</li> <li>• Verify that the connection failed via log</li> </ul>
<b>Expected Test Results</b>	Verify with logs that when an incomplete certificate trust chain is present, the TOE is not able to make a successful connection
<b>Pass/Fail with Explanation</b>	Pass. When an incomplete certificate trust chain is present, the TOE is not able to make a successful connection. This meets the testing requirements.

## FIA\_X509\_EXT.1.1/Rev Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>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.</p> <p>Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• For TOE configurations, refer to FIA_X509_EXT.1.1 Test #1</li> <li>• Create a certificate that is expired according to the TOE</li> <li>• Attempt the TLS connection using expired certificate</li> <li>• Verify the connection is refused via packet capture</li> <li>• Verify the connection is refused via logs</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the evaluator should verify that validating an expired certificate resulted in function failing
<b>Pass/Fail with Explanation</b>	Pass. The evaluator verified that validating an expired certificate resulted in function failing. This meets the testing requirements

## FIA\_X509\_EXT.1.1/Rev Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>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.</p> <p>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.</p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the trustpoint for Root CA and authenticate the certificate (Here default CRL check is ON)</li> <li>• Configure the trustpoint for intermediate certificate (Here default CRL check is ON)</li> <li>• Configure the TLS over syslog connection</li> <li>• Create a signed certificate for the server</li> <li>• Attempt to establish a TLS connection (connection will pass)</li> <li>• Verify that the session completes via logs</li> <li>• Verify the downloaded CRLs on the TOE</li> <li>• Verify that the session completes via packet capture</li> <li>• Revoke the server's certificate and upload the CRL onto the apache server</li> <li>• Attempt to establish a TLS connection (connection will fail)</li> <li>• Verify the failure logs</li> <li>• Verify the downloaded CRLs on the TOE</li> <li>• Verify the pcap</li> <li>• Unrevoke the server certificate</li> <li>• Revoke the intermediate certificate and upload the CRL onto the TOE</li> </ul>



	<ul style="list-style-type: none"> <li>• Attempt to establish a TLS connection (connection will fail)</li> <li>• Verify the failure logs</li> <li>• Verify the downloaded CRLs on the TOE</li> <li>• Verify with the pcap</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the TOE communications with peers will fail that either have a revoked certificate or one of their intermediary CA certificates are revoked. When presented non-revoked certificates, the TOE accepts should the connection
<b>Pass/Fail with Explanation</b>	Pass. The TOE communications with peers will fail that either have a revoked certificate or one of their intermediary CA certificates are revoked. When presented non-revoked certificates, the TOE accepts the connection. This meets the testing requirements

#### FIA\_X509\_EXT.1.1/Rev Test #4

Item	Data
<b>Test Assurance Activity</b>	<p>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.</p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create the intermediate CA with CRL sign bit OFF</li> <li>• Make sure that CA certificates are uploaded onto the TOE</li> <li>• Make sure that CRL check is ON onto the TOE</li> <li>• Create the server certificate signed by the ICA which does not have CRL sign bit</li> <li>• Attempt TLS connection with syslog server</li> <li>• Verify the pcap</li> <li>• Verify the failure logs</li> </ul>

<b>Expected Test Results</b>	Verify with logs that TOE fails to validate the intermediate CA certificate when CRL sign usage bit is not present in the certificate
<b>Pass/Fail with Explanation</b>	Pass. TOE fails to validate the intermediate CA certificate when CRL sign usage bit is not present in the certificate. This meets the testing requirements.

### FIA\_X509\_EXT.1.1/Rev Test #5

Item	Data
<b>Test Assurance Activity</b>	<p>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.</p> <p>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.)</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• For TOE configurations, refer FIA_X509_EXT.1.1 Test #1</li> <li>• A connection will start between the TOE and TLS.</li> <li>• Verify the connection is refused via packet capture</li> <li>• Verify the connection is refused via log</li> </ul>
<b>Expected Test Results</b>	Verify with logs that TLS connection was rejected when first eight bytes will modify
<b>Pass/Fail with Explanation</b>	Pass. TLS connection was rejected when first eight bytes were modified. This meets the requirement.

### FIA\_X509\_EXT.1.1/Rev Test #6

Item	Data
<b>Test Assurance Activity</b>	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.)
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• For TOE configurations, refer FIA_X509_EXT.1.1 Test #1</li> <li>• A connection will start between the TOE and TLS</li> <li>• Verify the connection is refused via packet capture</li> <li>• Verify the connection is refused via logs</li> </ul>
<b>Expected Test Results</b>	Verify with logs that TLS connection will reject when last bytes will modify
<b>Pass/Fail with Explanation</b>	Pass. TLS connection was rejected when last bytes were modified. This meets the requirement.

### **FIA\_X509\_EXT.1.1/Rev Test #7**

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	<p>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.</p> <p>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.)</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• For TOE configurations, refer FIA_X509_EXT.1.1 Test #1</li> <li>• A connection will start between the TOE and TLS</li> <li>• Verify the connection is refused via packet capture</li> <li>• Verify the connection is refused via logs</li> </ul>
<b>Expected Test Results</b>	Verify with logs that TLS connection will reset when bytes in public key will modify

<b>Pass/Fail with Explanation</b>	Pass. TLS connection was reset when bytes in public key were modified. This meets the requirement.
-----------------------------------	--

## FIA\_X509\_EXT.1.2/Rev Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>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.</p> <p>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).</p> <p>For each of the following tests the evaluator shall create a chain of at least three certificates:</p> <ul style="list-style-type: none"> <li>- a self-signed root CA certificate,</li> <li>- an intermediate CA certificate and</li> <li>- a leaf (node) certificate.</li> </ul> <p>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).</p> <p>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:</p> <ul style="list-style-type: none"> <li>(i) <i>as part of the validation of the leaf certificate belonging to this chain;</i></li> <li>(ii) <i>(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).</i></li> </ul>

<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create ICA certificate without basic Constraint</li> <li>• Try to authenticate the ICA certificate onto the TOE</li> <li>• Verify the failure logs</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the TOE rejects the ICA when CA bit is not set should pass
<b>Pass/Fail with Explanation</b>	Pass. TOE rejects the ICA when CA bit is not set. This meets the requirement.

## FIA\_X509\_EXT.1.2/Rev Test #2

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	<p>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.</p> <p>The goal of the following tests is 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).</p> <p>For each of the following tests the evaluator shall create a chain of at least three certificates:</p> <ul style="list-style-type: none"> <li>- a self-signed root CA certificate,</li> <li>- an intermediate CA certificate and</li> <li>- a leaf (node) certificate.</li> </ul> <p>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).</p> <p>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:</p> <p>(i) As part of the validation of the leaf certificate belonging to this chain;</p>

	(ii) 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).
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create ICA with basic constraint false</li> <li>• Try to authenticate the ICA certificate onto the TOE</li> <li>• Verify the failure logs</li> </ul>
<b>Expected Test Results</b>	Verify with logs that TOE rejects the ICA basic constraint of CA is set to false
<b>Pass/Fail with Explanation</b>	Pass. TOE rejects the ICA basic constraint of CA is set to false. This meets the requirement.

## FIA\_X509\_EXT.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following test for each trusted channel:</p> <p>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.</p> <p>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.</p> <p>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.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the trustpoint for AcumenCA and authenticate the certificate (Here default CRL check is ON)</li> <li>• Configure the trustpoint for intermediate certificate (Here default CRL check is ON)</li> <li>• Configure the TOE for TLS over syslog connection`</li> <li>• Create a signed certificate for server</li> <li>• Attempt to make a TLS connection (connection will pass)</li> <li>• Verify that the session completes via logs</li> <li>• Verify the downloaded CRLs on the TOE</li> <li>• Verify that the session completes via packet capture</li> </ul>

	<ul style="list-style-type: none"> <li>• On the server, disable the httpd service</li> <li>• Attempt to make a connection (connection will fail)</li> <li>• Verify the reason for failure via logs</li> <li>• Verify that the session failure via packet capture</li> </ul>
<b>Expected Test Results</b>	Verify with logs that TOE does not accept the connection when crl server is disabled
<b>Pass/Fail with Explanation</b>	Pass. TOE does not accept the connection when crl server is disabled. This meets the requirements.

### FIA\_X509\_EXT.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• From the TOE, generate a CSR</li> <li>• Examine the CSR contents</li> <li>• Ensure the CSR contains the following fields <ul style="list-style-type: none"> <li>○ <i>Public Key</i></li> <li>○ <i>CN</i></li> </ul> </li> </ul>
<b>Expected Test Results</b>	Verify with logs that TOE is able generate the CSR and CSR contains all required information should pass
<b>Pass/Fail with Explanation</b>	Pass. TOE is able generate the CSR and CSR contains all required information. This meets the testing requirements.

## FIA\_X509\_EXT.3 Test #2

Item	Data
<b>Test Assurance Activity</b>	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.
<b>Test Steps</b>	<ul style="list-style-type: none"><li>• From the TOE, generate a CSR request</li><li>• Generate a signed certificate based on the generated CSR from an external CA</li><li>• Delete an intermediate certificate</li><li>• Attempt to load the signed certificate on the TOE. Verify that the TOE rejects the certificate because the full trust chain of the CA is not present</li><li>• Add the intermediary certificates to the TOE certificate store to ensure that the signing CA now has a full certificate path</li><li>• Re-attempt to load the signed certificate on the TOE</li><li>• Verify that the TOE accepts the certificate because the path validation succeeded</li></ul>
<b>Expected Test Results</b>	Verify with logs that the TOE does not install CSR responses signed by a CA without a full trust path & the TOE does install a CSR response signed by a CA with a full trust path
<b>Pass/Fail with Explanation</b>	Pass. The TOE does not install CSR responses signed by a CA without a full trust path. The TOE does install a CSR response signed by a CA with a full trust path. This meets the testing requirements.

## 15.1.6 MACsec

### FAU\_GEN.1/MACSEC Test #1

Item	Data
------	------



<b>Test Assurance Activity</b>	The evaluator shall complete the assurance activity for FAU_GEN.1 as described in the NDcPP for the auditable events defined above in addition to the applicable auditable events that are defined in the NDcPP. The evaluator shall also ensure that the administrative actions defined for this EP are appropriately audited.
<b>Pass/Fail with Explanation</b>	Pass. This test is covered by FAU_GEN (NDcPP).

### FCS\_MACSEC\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall successfully establish a MACsec channel between the TOE and a MACsec-capable peer in the Operational Environment and verify that the TSF logs the communications. The evaluator shall capture the traffic between the TOE and the Operational Environment to determine the SCI that the TOE uses to identify the peer. The evaluator shall then configure a test system to capture traffic between the peer and the TOE to modify the SCI that is used to identify the peer. The evaluator then verifies that the TOE does not reply to this traffic and logs that the traffic was discarded
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE to use MACsec.</li> <li>• Configure the PEER to use MACsec.</li> <li>• Attempt a connection and verify that it is successful.</li> <li>• Verify via packet capture.</li> <li>• Verify via logs.</li> <li>• Use MACsec testing tool to modify SCI of traffic from peer.</li> <li>• Check the PCAP for modified packets. Also note the lack of reply packets from TOE.</li> </ul>
<b>Expected Test Results</b>	Verify with logs that Successful MACsec connection should established, and during mod sci test, modified SCI packets were rejected by the TOE

<b>Pass/Fail with Explanation</b>	Pass. Successful MACsec connection was established, and during modsci test, modified SCI packets were rejected by the TOE. This meets the testing requirements.
-----------------------------------	---

## FCS\_MACSEC\_EXT.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall send Ethernet traffic to the TOE's MAC address that iterates through the full range of supported EtherType values (refer to <a href="http://standards.ieee.org/develop/regauth/ethertype/eth.txt">http://standards.ieee.org/develop/regauth/ethertype/eth.txt</a> ) and observes that traffic for all EtherType values is discarded by the TOE except for the traffic which has an EtherType value of 88-8E, 88-E5 or 8808. Note that there are a large number of EtherType values so the evaluator is encouraged to execute a script that automatically iterates through each value.  <b>TD0553 has been applied.</b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• <b>Start the MACsec tool to send a variety of EtherTypes.</b></li> <li>• <b>The PCAP shows various EtherTypes sent with NO reply from the TOE.</b></li> <li>• <b>Packet with EtherType value of 88-8E, 88-E5 or 8808 are accepted by the TOE.</b></li> </ul>
<b>Expected Test Results</b>	Verify with logs that EtherTypes other than value of 88-8E, 88-E5 or 8808 should be rejected by the TOE.
<b>Pass/Fail with Explanation</b>	Pass. EtherTypes other than 88-8E and 88-E5 are rejected by the TOE. Although the EtherType 8808 (control frames) are allowed by the requirement to be accepted, the TOE's default behavior is to discard the 8808 EtherType. This meets the testing requirements.

## FCS\_MACSEC\_EXT.2 Test #1

Item	Data
------	------

<b>Test Assurance Activity</b>	The evaluator shall transmit MACsec traffic to the TOE from a MACsec-capable peer in the Operational Environment. The evaluator shall verify via packet captures and/or audit logs that the frame bytes after the MACsec Tag values in the received traffic is not obviously predictable.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration</li> <li>• Acquire PCAP of a successful MACsec connection</li> <li>• Verify in PCAP that MACsec packets is not obviously predictable</li> </ul>
<b>Expected Test Results</b>	Verify with logs that Bytes following the MACsec tag in the MKPDUs are not obviously predictable
<b>Pass/Fail with Explanation</b>	Pass. Bytes following the MACsec tag in the MKPDUs are not obviously predictable. This meets the testing requirements.

## FCS\_MACSEC\_EXT.2 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall transmit valid MACsec traffic to the TOE from a MACsec-capable peer in the operational environment that is routed through a test system set up as a man-in-the-middle. The evaluator shall use the test system to intercept this traffic to modify one bit in a packet payload before retransmitting to the TOE. The evaluator shall verify that the traffic is discarded due to an integrity failure.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration</li> <li>• Use the MACsec tool to modify a bit in a packet payload</li> <li>• Check the PCAP for modified packets. Note that no reply from the TOE was detected</li> </ul>
<b>Expected Test Results</b>	Verify with logs that modified ICV packets are rejected by the TOE

<b>Pass/Fail with Explanation</b>	Pass. Modified ICV packets are rejected by the TOE. This meets the testing requirements.
-----------------------------------	--

## FCS\_MACSEC\_EXT.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>For each supported method of peer authentication in FCS_MACSEC_EXT.4.1, the evaluator shall follow the operational guidance to configure the supported method (if applicable).</p> <p>The evaluator shall set up a packet sniffer between the TOE and a MACsec-capable peer in the Operational Environment. The evaluator shall then initiate a connection between the TOE and the peer such that authentication occurs and a secure connection is established. The evaluator shall wait 1 minute and then disconnect the TOE from the peer and stop the sniffer.</p> <p>The evaluator shall use the packet captures to verify that the secure channel was established via the selected mechanism and that the EtherType of the first data frame sent between the TOE and the peer is 88-E5.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration</li> <li>• Start a new session and keep it on for 1 minute</li> <li>• Observe the PCAP. The first packet has EtherTypes of 88e5</li> <li>• Verify the logs</li> </ul>
<b>Expected Test Results</b>	<p>Verify with logs that Secure channel should established between the TOE and peer.</p> <p>88E5 was first data packet between TOE and peer should pass</p>
<b>Pass/Fail with Explanation</b>	Pass. Secure channel was established between the TOE and peer. 88E5 was first data packet between TOE and peer. This meets the testing requirements.

## FCS\_MACSEC\_EXT.4 Test #2

Item	Data
------	------

<b>Test Assurance Activity</b>	The evaluator shall capture traffic between the TOE and a MACsec-capable peer in the Operational Environment. The evaluator shall then cause the TOE to distribute a SAK to that peer, capture the MKPDUs from that operation, and verify the key is wrapped in the captured MKPDUs.  <i>TD0273 Applied.</i>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE for MACsec so that TOE will send distributed SAK to peer</li> <li>• Configure the peer for MACsec</li> <li>• Ping the peer</li> <li>• Observe in PCAP for Distributed SAK</li> <li>• Verify the logs</li> </ul>
<b>Expected Test Results</b>	Verify with logs that the AES key is wrapped in the captured MKPDUs should pass
<b>Pass/Fail with Explanation</b>	Pass. The AES key is wrapped in the captured MKPDUs. This meets the testing requirements.

## FCS\_MKA\_EXT.1.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The test below requires the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following test:</p> <p>The evaluator shall use a peer device to send traffic to the TOE, arbitrarily inducing artificial delays in their transmission using a man-in-the-middle setup. The evaluator shall observe that traffic delayed longer than 2.0 seconds is rejected.</p> <p><i>TD0618 has been applied.</i></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MKA_EXT.1.5 Test #1 test case for configuration</li> <li>• Use the MACsec tool to inject delays into traffic transmission</li> <li>• Observer PCAP, the delay causes the channel to fail</li> </ul>

<b>Expected Test Results</b>	Verify with packet capture that after delay, the MACsec connection broke should pass
<b>Pass/Fail with Explanation</b>	Pass. After a delay, the MACsec connection broke. This meets the testing requirements.

### FCS\_MKA\_EXT.1.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall transmit MKA traffic (MKPDUs) to the TOE from a MKA-capable 21 peer in the Operational Environment. The evaluator shall verify via packet captures and/or audit logs that the last 16 octets of the MKPDUs in the received traffic do not appear to be predictable.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Acquire PCAP of a good MACsec connection</li> <li>• Observe the last 16 octets of MKA frame. They are in an unpredictable sequence</li> </ul>
<b>Expected Test Results</b>	Verify with packet capture that the last 16 octets of a given MKA frame is in an unpredictable sequence should pass
<b>Pass/Fail with Explanation</b>	Pass. The last 16 octets of a given MKA frame is in an unpredictable sequence. This meets the testing requirements.

### FCS\_MKA\_EXT.1.4 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall transmit valid MKA traffic to the TOE from a MKA-capable peer in the operational environment that is routed through a test system set up as a man-in-the-middle. The evaluator shall use the test system to intercept this traffic to modify one bit in a packet payload before retransmitting to the TOE. The evaluator shall verify that the traffic is discarded due to an integrity failure.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration</li> <li>• Run the MACsec tool to modify a frame byte in transit</li> </ul>

	<ul style="list-style-type: none"> <li>Examine the PCAP. Note how the packet is modified</li> </ul>
<b>Expected Test Results</b>	Verify with packet capture that Modified MKA packets were rejected by the TOE
<b>Pass/Fail with Explanation</b>	Pass. Modified MKA packets were rejected by the TOE. This meets the testing requirements.

## FCS\_MKA\_EXT.1.5 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with.</p> <p>Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor (peer). The evaluator shall then perform the following tests using a traffic sniffer to capture this traffic.</p> <p>Test 1: The evaluator shall send a fresh SAK that includes both peers as active participants. The evaluator shall start an MKA session between the TOE and the two active participant peers and send MKPDUs. The evaluator shall verify from packet captures that MKPDUs are sent at least once every half-second.</p> <p><b><i>TD0618 has been applied.</i></b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Show that the TOE, Peer B &amp; Peer C is configured for MACsec session</li> <li>Clear previous MACsec sessions.</li> <li>Start the MACsec connection with Peer B.</li> <li>Verify from the Packet Capture that the MKA packets are sent every 0.5 seconds.</li> <li>Start the MACsec connection with Peer C</li> <li>Verify from the Packet Capture that the MKA packets are sent every 0.5 seconds</li> <li></li> </ul>
<b>Expected Test Results</b>	Verify with pcap that MKA packets should send regularly every half a second

<b>Pass/Fail with Explanation</b>	Pass. MKA packets are sent regularly every half a second. This meets the testing requirements.
-----------------------------------	--

## FCS\_MKA\_EXT.1.5 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with.</p> <p>Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor (peer). The evaluator shall then perform the following tests using a traffic sniffer to capture this traffic.</p> <p>Test 2: Disconnect one of the peers. Using a man-in-the-middle device, arbitrarily introduce an artificial delay in sending a fresh SAK following the change in the Live Peer List. Repeat Test 1 delaying a fresh SAK for MKA Lifetime traffic and observe that the timeout of 6.0 seconds is enforced by the TSF.</p> <p><b><i>TD0618 has been applied.</i></b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• For TOE configurations, refer FCS_MKA_EXT.1.5 Test #1</li> <li>• Run the MACsec tool that will delay the distributed SAK file, then restart the MACsec connection</li> <li>• Examine the PCAP. The Test begins at Packet #60. Six seconds later, highlighted is the delayed SAK packet, resulting in the connection failing.</li> </ul>
<b>Expected Test Results</b>	Verify with PCAP that traffic delayed over 6 seconds causes the MACsec connection to fail
<b>Pass/Fail with Explanation</b>	Pass. Traffic delayed over 6 seconds causes the MACsec connection to fail. This meets the testing requirements.



## FCS\_MKA\_EXT.1.8 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 1 [conditional]: If the TOE supports group CAKs, The evaluator shall perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Load one PSK onto the TOE and device B and a second PSK onto the TOE and device C. This defines two pairwise CAs.</li> <li>2. Generate a group CAK for the group of 3 devices using <code>ieee8021XKayCreateNewGroup</code>.</li> <li>3. Observe via packet capture that the TOE distributes the group CAK to the two peers, protected by AES key wrap using their respective PSKs.</li> <li>4. Verify that B can form a SA with C and connect securely.</li> <li>5. Disable the KaY functionality of device C using <code>ieee8021XPaePortKayMkaEnable</code>.</li> <li>6. Generate a group CAK for the TOE and B using <code>ieee8021XKayCreateNewGroup</code> and observe they can connect.</li> <li>7. The evaluator shall have B attempt to connect to C and observe this fails.</li> <li>8. Re-enable the KaY functionality of device C.</li> <li>9. Invoke <code>ieee8021XKayCreateNewGroup</code> again.</li> <li>10. Verify that both the TOE can connect to C and that B can connect to C.</li> </ol> <p><b><i>TD0618 has been applied.</i></b></p>
<b>Pass/Fail with Explanation</b>	<p>N/A. As per ST SFR, Group CAKs for establishing multiple MKA connections is not claimed.</p>

## FCS\_MKA\_EXT.1.8 Test #2a

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Send an MKPDU to the TOE's individual MAC address from a peer. Verify the frame is dropped and logged.</li> </ol> <p><b><i>TD0618 has been applied.</i></b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MKA_EXT.1.5 Test #1 test case for configuration</li> <li>• Use the MACsec tool to send traffic to the individual MAC address of the TOE</li> <li>• The PCAP shows that the delivered packet is ignored by the TOE with no reply</li> <li>• Verify the logs</li> </ul>
<b>Expected Test Results</b>	Traffic send to the individual Mac address of the TOE should reject by the TOE
<b>Pass/Fail with Explanation</b>	Pass. All modified packets are dropped by TOE. This meets the testing requirements.

## FCS\_MKA\_EXT.1.8 Test #2b

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:</p> <ol style="list-style-type: none"> <li>2. Send an MKPDU to the TOE that is less than 32 octets long. Verify the frame is dropped and logged.</li> </ol>

	<b><i>TD0618 has been applied.</i></b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MKA_EXT.1.5 Test #1 test case for configuration</li> <li>• Use the MACsec tool to send packets less than 32 octets long</li> <li>• The PCAP shows the modified packets are ignored</li> </ul>
<b>Expected Test Results</b>	Packet send to the TOE which is less than 32 octets should reject by the TOE
<b>Pass/Fail with Explanation</b>	Pass. MKPDU packets lesser than 32 octets are rejected by the TOE. This meets the testing requirements.

### **FCS\_MKA\_EXT.1.8 Test #2c**

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:</p> <p>3. Send an MKPDU to the TOE whose length in octets is not a multiple of 4. Verify the frame is dropped and logged.</p> <p><b><i>TD0618 has been applied.</i></b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MKA_EXT.1.5 Test #1 test case for configuration</li> <li>• Use the MACsec tool to send packets whose octets are not a multiple of 4</li> <li>• The PCAP shows the modified packets are ignored</li> <li>• Verify the logs</li> </ul>
<b>Expected Test Results</b>	Packet send to the TOE whose octets are not multiple of 4 should reject by TOE
<b>Pass/Fail with Explanation</b>	Pass. MKPDU sent to the TOE whose length in octets is not a multiple of 4 are dropped by the TOE. This meets the testing requirements.

## FCS\_MKA\_EXT.1.8 Test #2d

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:</p> <p>4. Send an MKPDU to the TOE that is one byte short. Verify the frame is dropped and logged.</p> <p><b><i>TD0618 has been applied.</i></b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MKA_EXT.1.5 Test #1 test case for configuration</li> <li>• Use the MACsec tool to send MKPDU packets whose length are one byte short</li> <li>• The PCAP shows the modified packets are rejected</li> <li>• Verify the logs</li> </ul>
<b>Expected Test Results</b>	Single byte short in the MKPDU should dropped the packet by the TOE
<b>Pass/Fail with Explanation</b>	Pass. MKPDU sent to the TOE that is one byte short are dropped by the TOE. This meets the testing requirements.

## FCS\_MKA\_EXT.1.8 Test #2e

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:</p>

	5. Send an MKPDU to the TOE with unknown Agility Parameter. Verify the frame is dropped and logged.  <i>TD0618 has been applied.</i>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MKA_EXT.1.5 Test #1 test case for configuration</li> <li>• Use MACsec tool to send MKPDU packet with unknown agility parameters</li> <li>• The PCAP shows the modified packets are rejected</li> <li>• Verify the logs</li> </ul>
<b>Expected Test Results</b>	Packets with unknown agility parameters should dropped by the TOE
<b>Pass/Fail with Explanation</b>	Pass. Packets with unknown Agility Parameter are dropped by the TOE. This meets the testing requirements.

## FIA\_AFL.1/MACSEC Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall perform the following tests for each method by which remote administrators access the TOE:  Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE. The evaluator shall test that once the limit is reached for a given remote administrator account, subsequent attempts with valid credentials are not successful.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Login into the TOE via SSH</li> <li>• Set the TOE to lock out a user after five failed attempts</li> <li>• Starting login attempts with bad password “asdmhtgbhkly”.</li> <li>• Checking that we can’t login with good password “123Test321”; Verifying that user is locked</li> <li>• Verify the logs</li> </ul>
<b>Expected Test Results</b>	Unsuccessful attempt to login into the TOE will lock the user
<b>Pass/Fail with Explanation</b>	Pass. The TOE did not allow authentication once the authentication attempt limit has been reached. This meets the testing requirements.

### FIA\_AFL.1/MACSEC Test #3

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall perform the following tests for each method by which remote administrators access the TOE:  [conditional] If the TSS indicates that an administrator-configurable time period must elapse in order to automatically re-enable an account that was locked out due to excessive authentication failures, the evaluator shall perform the steps in Test 1 to lock out an account, follow the operational guidance to configure a time period of their choosing, and observe through periodic login attempts that the account cannot successfully log in until the configured amount of time has elapsed. The evaluator shall then repeat this test for a different time period of their choosing.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Login into the TOE via SSH</li> <li>• Set the TOE to lock out a user after five failed attempts &amp; lockout time period 5 min</li> <li>• Starting login attempts with bad password “asdmhtgbhkly”.</li> <li>• Checking that we can’t login with good password “123Test321”; Verifying that user is locked</li> <li>• Verify with the logs</li> <li>• Wait for more than 5 minutes and try to login into the TOE; This will pass</li> <li>• Verify with the logs</li> </ul>
<b>Expected Test Results</b>	Verify with logs that unsuccessful attempt to login into TOE will lock the user & unlock after few minutes
<b>Pass/Fail with Explanation</b>	Pass. User is able to login into the TOE when configured time period is elapsed. This meets the testing requirements.

### FIA\_PSK\_EXT.1/MACSEC Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.

	Test 1 [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall use the minimum length; the maximum length; a length inside the allowable range; and invalid lengths beyond the supported range (both higher and lower). The minimum, maximum, and included length tests should be successful, and the invalid lengths must be rejected by the TOE.
<b>Test Steps</b>	<p>128-bit key</p> <ul style="list-style-type: none"> <li>• Attempt to input a 31 character key. This is rejected</li> <li>• Attempt to input a 32 character key. This is accepted</li> <li>• Attempt to input a 38 character key. This is rejected</li> </ul> <p>256-bit key</p> <ul style="list-style-type: none"> <li>• Attempt to input a 40 character key. This is rejected</li> <li>• Attempt to input a 64 character key. This is accepted</li> <li>• Attempt to input a 68 character key. This is rejected</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Proper length keys should accept and improper length keys should reject by TOE</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Proper length keys were accepted, and improper keys rejected. This meets the testing requirements.

## FIA\_PSK\_EXT.1/MACSEC Test #2

<b>Item</b>	<b>Data</b>
<b>Test Assurance Activity</b>	<p>The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.</p> <p>Test 2 [conditional]: If the TOE does not <b>generate</b> bit-based pre-shared keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.</p>
<b>Test Steps</b>	256 bits

	<ul style="list-style-type: none"> <li>• Enter the generated key into the macsec policy on both the peer and the TOE</li> <li>• Verify that a connection can be established</li> <li>• The TOE allowed for a connection when using the randomly generated password. This is indicated by the secured MKA session with MACsec</li> <li>• Verify via packet capture</li> <li>• Verify via logs</li> </ul> <p>128 bits</p> <ul style="list-style-type: none"> <li>• Enter the generated key into the macsec policy on both the peer and the TOE</li> <li>• Verify that a connection can be established</li> <li>• The TOE allowed for a connection when using the randomly generated password. This is indicated by the secured MKA session with MACsec</li> <li>• Verify via packet capture</li> <li>• Verify via logs</li> </ul>
<b>Expected Test Results</b>	Generated key should be used in a successful MACsec connection
<b>Pass/Fail with Explanation</b>	Pass. The entered key will be used in a successful MACsec connection. This meets the testing requirements.

### FIA\_PSK\_EXT.1/MACSEC Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.</p> <p>Test 3 [conditional]: If the TOE does <b>generate</b> bit-based pre-shared keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.</p>



<b>Pass/Fail with Explanation</b>	NA. TOE does generate bit-based pre-shared keys.
-----------------------------------	--

## FMT\_SMF.1/MACSEC Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall set up an environment where the TOE can connect to two other MACsec devices, identified as devices B and C, with the ability of pre-shared keys to be distributed between them. The evaluator shall configure the devices so that the TOE will be elected key server and principal actor, i.e., has highest key server priority.</p> <p>In addition to the tests specified in the NDcPP for this SFR, the evaluator shall follow the relevant operational guidance to perform the tests listed below. Note that if the TOE claims multiple management interfaces, the tests should be performed for each interface that supports the functions.</p> <p>Test 1: The evaluator shall connect to the PAE of the TOE and install a PSK. The evaluator shall then specify a CKN and that the PSK is to be used as a CAK.</p> <ul style="list-style-type: none"> <li>• Repeat this test for both 128-bit and 256-bit key sizes.</li> <li>• Repeat this test for a CKN of valid length (1-32 octets), and observe success.</li> <li>• Repeat this test again for CKN of invalid lengths zero and 33, and observe failure.</li> </ul> <p><b>TD0652 has been applied.</b></p>
<b>Test Steps</b>	<p>128-bit:</p> <ul style="list-style-type: none"> <li>• Attempt to set a 128-bit key (32 characters). This will succeed.</li> <li>• Confirm keys in config</li> <li>• Attempt a key of length 0. This will fail.</li> <li>• Attempt to set a key that is 33 characters in length. This will fail.</li> </ul> <p>256-bit:</p> <ul style="list-style-type: none"> <li>• Attempt to set a 256-bit key (64 characters). This will succeed.</li> <li>• Confirm keys in config</li> </ul>

	<ul style="list-style-type: none"> <li>Attempt a key of length 0. This will fail.</li> </ul> <p>Attempt to set a key that is 65 characters in length. This will fail.</p>
<b>Expected Test Results</b>	Keys send to the TOE with good length should accepted by TOE but should reject bad length keys
<b>Pass/Fail with Explanation</b>	Pass. Good length keys were accepted by the TOE, bad length keys were rejected by the TOE. This meets the testing requirements.

## FMT\_SMF.1/MACSEC Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall set up an environment where the TOE can connect to two other MACsec devices, identified as devices B and C, with the ability of pre-shared keys to be distributed between them. The evaluator shall configure the devices so that the TOE will be elected key server and principal actor, i.e., has highest key server priority.</p> <p>In addition to the tests specified in the NDcPP for this SFR, the evaluator shall follow the relevant operational guidance to perform the tests listed below. Note that if the TOE claims multiple management interfaces, the tests should be performed for each interface that supports the functions.</p> <p>The evaluator will test the ability of the TOE to enable and disable MKA participants using the management function specified in the ST.</p> <p>The evaluator shall install pre-shared keys in devices B and C, and take any necessary additional steps to create corresponding MKA participants. The evaluator shall disable the MKA participant on device C, then observe that the TOE can communicate with B but neither the TOE nor B can communicate with device C. The evaluator shall re-enable the MKA participant of device B and observe that the TOE is now able to communicate with devices B and C.</p> <p><b>TD0652 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Start MACsec connection with TOE, Peer B, and Peer C</li> <li>Confirm that Peer B and communicate with C directly</li> <li>Disable MACsec on Peer C</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify that the TOE can communicate with Peer B but not with C</li> <li>• Similarly, B cannot communicate with C</li> <li>• Turn MACsec back on for Peer C</li> <li>• Verify all the connections are good</li> </ul>
<b>Expected Test Results</b>	The TOE should stop the connection with peer if the peer turn off.
<b>Pass/Fail with Explanation</b>	Pass. When a non-TOE peer turns off the MACsec configuration, the TOE doesn't accept the traffic. Once the macsec is enabled on the peer, secured channel was established between the TOE and peer. This meets testing requirement.

### FMT\_SMF.1/MACSEC Test #3a

Item	Data
<b>Test Assurance Activity</b>	<p>For TOEs using only PSKs, the TOE should be the Key Server in both tests and only one peer (B) needs to be tested.</p> <p>The tests are:</p> <p>Subtest a (Switch to unexpired CKN): TOE and Peer B have CKN1(10 minutes) and CKN2. CKN2 can either be configured with a longer overlapping lifetime (20 minutes) or be configured with a lifetime starting period of more than 10 minutes after the CKN1 start. The TOE and Peer B start using CKN1 and after 10 minutes, verify that the TOE expires SAK1. This can be verified by either 1) seeing the TOE immediately distribute a new SAK to the peer if the lifetime of CKN2 overlaps CKN1, or 2) by terminating the connection with CKN1 and distributing a new SAK once the lifetime period of CKN2 begins.</p> <p><b>TD0652 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The TOE has a lifetime of 10 minutes on key 1234 and a lifetime of 20 minutes on key 3456</li> <li>• The Peer has a lifetime of 10 minutes on key 1234 and a lifetime of 20 minutes on key 3456</li> <li>• Verify the connection and time</li> <li>• Verify that the session is using key 1234</li> <li>• Verify via logs that the session is using key 1234 for 10 mins</li> <li>• Verify via packet capture that the session is using key 1234</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify after 10 mins that the session uses key 3456</li> <li>• Verify via logs after 10 mins that the session uses key 3456</li> <li>• Verify via packet capture after 10 mins that the session uses key 3456</li> </ul>
<b>Expected Test Results</b>	<p>TOE need to be configured with a second key in the chain.</p> <p>The connection will delete the request from the peer and renegotiate with the new CAK.</p>
<b>Pass/Fail with Explanation</b>	<p>Pass. The test performs re-keying at the configured time when the TOE is configured with a second key in the chain. The connection will delete the request from the peer and renegotiate with the new CAK. This meets the testing requirements.</p>

### FMT\_SMF.1/MACSEC Test #3b

Item	Data
<b>Test Assurance Activity</b>	<p>Test 3: For TOEs using only PSKs, the TOE should be the Key Server in both tests and only one peer (B) needs to be tested.</p> <p>The tests are:</p> <p>Subtest b (reject CA with expired CKN): TOE has CKN1(10 minutes). Peer B has CKN1(20 minutes). TOE and Peer B start using CKN1 and after 10 minutes, verify that the TOE rejects (or ignores) peer's request to use (or distribute a) SAK using CKN1.</p> <p><b>TD0652 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• The TOE has a lifetime of 10 minutes on key 1234 and a lifetime of 20 minutes on key 5678</li> <li>• The peer has a lifetime of 20 minutes only on key 1234</li> <li>• Verify the time</li> <li>• Verify that the session is using key 1234</li> <li>• Verify via packet capture that the session is using key 1234</li> <li>• Verify via logs that the session is using key 1234 for 10 mins</li> <li>• After the first CKN expires, the TOE switches to the next valid one. The connection fails because the peer still wants to use the old CKN</li> <li>• The PEER still uses CKN 1234 to establish the connection but since TOE is using CKN 5678 the connection fails due to mismatch</li> <li>• Verify the failure connection via logs</li> </ul>

<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>After expiring the key, TOE should reject the connection but peer will use same SAK.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejected a connection after the re-key occurred while the peer is still using the expired SAK. This meets the testing requirements.

### FMT\_SMF.1/MACSEC Test #4

Item	Data
<b>Test Assurance Activity</b>	<p>If “Cause Key Server to generate a new group CAK...” is selected, the evaluator shall connect to the PAE of the TOE, set the management function specified in the ST (e.g., set ieee8021XkeyCreateNewGroup to true), and observe that the TOE distributes a new group CAK.</p> <p><b>TD0652 has been applied.</b></p>
<b>Pass/Fail with Explanation</b>	<b>The TOE does not support group CAKs</b>

### FPT\_FLS.1(2)/SelfTest Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The following test may require the vendor to provide access to a test platform that provides the evaluator with the ability to modify the TOE internals in a manner that is not provided to end customers:</p> <p>Test 1: The evaluator shall modify the TSF in a way that will cause a self-test failure to occur. The evaluator shall determine that the TSF shuts down and that the behavior of the TOE is consistent with the operational guidance. The evaluator shall repeat this test for each type of self-test that can be deliberately induced to fail. For TOEs with redundant failover capability, the evaluator shall determine that the failed components shut down and the behavior of the TOE is consistent with the operational guidance. For each component, the evaluator shall repeat each type of self-test that can be deliberately induced to fail.</p> <p><b>TD0190 has been applied.</b></p>

<b>Test Steps</b>	<p>AES CMAC Failure:</p> <ul style="list-style-type: none"> <li>• Activate failure image on the TOE</li> <li>• Verify that boot image fails</li> </ul> <p>AES GCM Failure:</p> <ul style="list-style-type: none"> <li>• Verify that boot image fails</li> </ul> <p>DRBG Failure:</p> <ul style="list-style-type: none"> <li>• Verify that boot image fails</li> </ul> <p>HMAC Failure:</p> <ul style="list-style-type: none"> <li>• Verify that boot image fails</li> </ul> <p>SHA Failure:</p> <ul style="list-style-type: none"> <li>• Verify that boot image fails</li> </ul> <p>RSA Failure:</p> <ul style="list-style-type: none"> <li>• Verify that boot image fails</li> </ul> <p>Firmware Integrity Failure:</p> <ul style="list-style-type: none"> <li>• Verify that boot image fails</li> </ul>
<b>Expected Test Results</b>	<b>POST boot fails for Self test failure images</b>

<b>Pass/Fail with Explanation</b>	Pass. The TOE shuts down when a self-test failure occurs, and the behavior is consistent with the operational guidance. This meets the testing requirements.
-----------------------------------	--

## FPT\_RPL.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Before performing each test the evaluator shall successfully establish a MACsec channel between the TOE and a MACsec-capable peer in the Operational Environment sending enough traffic to see it working and verify the PN values increase for each direction</p> <p>Test 1: The evaluator shall set up a MACsec connection with an entity in the Operational Environment. The evaluator shall then capture traffic sent from this remote entity to the TOE. The evaluator shall retransmit copies of this traffic to the TOE in order to impersonate the remote entity where the PN values in the SecTag of these packets are less than the lowest acceptable PN for the SA. The evaluator shall observe that the TSF does not take action in response to receiving these packets and that the audit log indicates that the replayed traffic was discarded.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration</li> <li>• Verify the PN values increase for each direction</li> <li>• Record the lowest PN observed</li> <li>• Use MACsec tool to replay MACsec traffic from peer</li> <li>• Verify that repeated traffic is ignored, but normal traffic is fine</li> <li>• Verify that rejected traffic is logged</li> </ul>
<b>Expected Test Results</b>	Normal Traffic should be accepted by the TOE and repeated traffic should ignore by it.
<b>Pass/Fail with Explanation</b>	Pass. The TOE does not respond to replayed packets. This meets the testing requirements.

## FPT\_RPL.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Before performing each test the evaluator shall successfully establish a MACsec channel between the TOE and a MACsec-capable peer in the Operational Environment sending enough traffic to see it working and verify the PN values increase for each direction</p> <p>Test 2: The evaluator will capture frames during a MKA session and record the lowest PN observed in a particular time range. The evaluator will then send a frame with a lower PN, and then verify that this frame is dropped. The evaluator will verify that the device logged this event.</p>
<b>Test Output</b>	Covered by FPT_RPL.1 Test #1, where each duplicated encrypted ping has an invalid PN
<b>Pass/Fail with Explanation</b>	Pass. MKPDU replays are detected, discarded and logged. This meets the testing requirements.

## 16 Security Assurance Requirements

### 16.1.1 ADV\_FSP.1 Basic Functional Specification

#### ADV\_FSP.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	<p>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 of the Guidance Evaluation Activities.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass



## 16.1.2 AGD\_OPE.1 Operational User Guidance

### AGD\_OPE.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 shall 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 <a href="http://www.niap-ccevs.org">www.niap-ccevs.org</a> .  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

#### 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	<p>The evaluator ensured that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target. The section titled Supported Platforms of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are:</p> <table border="1"><tr><td>TOE Hardware Models</td><td>8808-SYS, 8812-SYS, 8818-SYS</td></tr><tr><td>TOE Software Version</td><td>IOS-XR 7.3</td></tr></table> <p>Based on these findings, this assurance activity is considered satisfied.</p>	TOE Hardware Models	8808-SYS, 8812-SYS, 8818-SYS	TOE Software Version	IOS-XR 7.3
TOE Hardware Models	8808-SYS, 8812-SYS, 8818-SYS				
TOE Software Version	IOS-XR 7.3				
Verdict	Pass.				

### 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.

### 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” & “Security Measures for the 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.

### AGD\_OPE.1 Activity 5 [TD0536]

Objective	In addition, the evaluator shall ensure that the following requirements are also met. <ul style="list-style-type: none"> <li>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.</li> <li>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: <ul style="list-style-type: none"> <li>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).</li> </ul> </li> </ul>
-----------	--

	<p>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.</p> <p>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.</p>
Evaluator Findings	<p>The evaluator verified the guidance documentation contains instructions for configuring any cryptographic engines in AGD_OPE.1 Test #3.</p> <p>The evaluator verified the guidance documentation describes the process for verifying updates in FPT_TUD_EXT.1 Guidance 2.</p> <p>The evaluator verified the guidance documentation makes it clear which security functionality is covered by the Evaluation Activities in AGD_OPE.1 Test #4.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 16.1.3 AGD\_PRE.1 Preparative Procedures

#### AGD\_PRE.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 “Security Measures for the Operational Environment” of the AGD. The evaluator found that these sections describe how the Operational Environment must meet:								
	<table border="1"> <thead> <tr> <th>Component</th> <th>Required</th> <th>Usage/Purpose Description for TOE performance</th> </tr> </thead> <tbody> <tr> <td>Management Workstation with SSH Client</td> <td>Yes</td> <td>This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support</td> </tr> </tbody> </table>	Component	Required	Usage/Purpose Description for TOE performance	Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support		
Component	Required	Usage/Purpose Description for TOE performance							
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support							

			TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
	Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
	MACsec Peer	Yes	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications.
	Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST
	Certificate Authority	Yes	This includes any Operational Environment Certificate Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
Based on these findings, this assurance activity is considered satisfied.			

Verdict	Pass.
---------	-------

AGD\_PRE.1 Activity 2

Objective	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.		
Evaluator Findings	The evaluator checked the requirements below 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 the guidance documentation describes each of the devices in the operating environment, including,		
	<b>Component</b>	<b>Required</b>	<b>Usage/Purpose Description for TOE performance</b>
	Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
	Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
	MACsec Peer	Yes	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that

		supports MACsec communications.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST
Certificate Authority	Yes	This includes any Operational Environment Certificate Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.

The section titled “Supported Hardware and Software” of AGD identifies the following supported platform:

**Table 1 Supported Hardware**

Hardware	Models
Cisco 8000 Series Routers	8808-SYS, 8812-SYS and 8818-SYS

**Table 2 Supported Software**

Software	Version
IOS XR	7.0

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

Verdict	Pass.
---------	-------

### 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	<p>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,</p> <ul style="list-style-type: none"><li>• Secure Installation and Configuration</li><li>• Secure Management</li><li>• Configuring Administrative Accounts and Passwords</li><li>• Configuring SSH and Console Connections</li><li>• Configuring the Remote Syslog Server</li><li>• Configuring Audit Log Options</li><li>• Configuring Event Logging</li><li>• Configuring a Secure Logging Channel</li></ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 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	<p>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.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### AGD\_PRE.1 Activity 5

Objective	In addition, the evaluator shall ensure that the following requirements are also met.
-----------	---

	<p>The preparative procedures must</p> <p>a) include instructions to provide a protected administrative capability; and</p> <p>b) identify TOE passwords that have default values associated with them and instructions shall be provided for how these can be changed.</p>
Evaluator Findings	<p>The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability and changing default passwords. The sections titled Passwords were used to determine the verdict of this work unit. The AGD describes changing the default password associated with the admin account and configuring password policy for TOE administration.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

#### 16.1.4 ALC Assurance Activities

##### ALC\_CMC.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	<p>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.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

##### ALC\_CMS.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	<p>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.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 16.1.5 ATE\_IND.1 Independent Testing – Conformance

#### ATE\_IND.1

##### ATE\_IND.1 Activity 1

Objective	<p>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.</p> <p>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.</p>
Evaluator Findings	<p>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.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

### 16.1.6 AVA\_VAN.1 Vulnerability Survey

#### AVA\_VAN.1

##### AVA\_VAN.1 Activity 1

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/vuln/search>
- <https://cve.mitre.org/>
- <http://www.kb.cert.org/vuls/html/search>
- <http://www.exploitsearch.net>
- <http://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>
- <https://tools.cisco.com/security/center/publicationListing.x> - Vendor Website

The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on 19 September 2022 and 23 October 2022.

The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. The list of keywords searched include:

- Cisco 8000 series
- C8000
- IOS XR 7.3
- Cisco IOS XR
- 8808-SYS
- 8812-SYS
- 8818-SYS
- 8808-RP
- 8808-FC
- 8812-FC
- 8818-FC
- 8800-LC-48H
- 8800-LC-36FH

	<ul style="list-style-type: none"> <li>• Intel Xeon D-1530 (Broadwell)</li> <li>• TLS 1.2</li> <li>• MACSEC</li> <li>• FIPS Object Module (FOM)</li> <li>• CoMIRA Mentor Questa</li> </ul> <p>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.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

AVA\_VAN.1 Activity 2

Objective	<p>The evaluator shall perform the following activities to generate type 4 flaw hypotheses:</p> <ul style="list-style-type: none"> <li>• Fuzz testing <ul style="list-style-type: none"> <li>○ Examine effects of sending: <ul style="list-style-type: none"> <li>▪ 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)</li> <li>▪ 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.</li> </ul> <p>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.</p> </li> <li>○ 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</li> </ul> </li> </ul>
-----------	--

	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	TOE does not accept improper packets. Based on the fuzz testing, the evaluator did not find any residual vulnerabilities which could be exploitable by an attacker with Basic Attack Potential.
Verdict	Pass.

## 17 Conclusion

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

**End of Document**