Assurance Activity Report for
Vertiv CYBEX™ SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM145DPH, SCM185DPH, SC985DPH, SCMV245DPH, SCMV285DPH Firmware Version 44444-E7E7 Peripheral Sharing Devices

Vertiv CYBEX™ SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM145DPH, SCM185DPH, SC985DPH, SCMV245DPH, SCMV285DPH Firmware Version 44444-E7E7 Peripheral Sharing Devices Security Target
Version 1.29, June 1, 2022

Protection Profile for Peripheral Sharing Device, Version: 4.0
PP-Module for Keyboard/Mouse Devices, Version 1.0
PP-Module for Video/Display Devices, Version 1.0
PP-Module for Analog Audio Output Devices, Version 1.0
PP-Module for User Authentication Devices, Version 1.0

AAR Version 1.4, June 1, 2022

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:
Vertiv
1050 Dearborn Dr.
Columbus, OH 43085

The Author of the Security Target:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

The TOE Evaluation was Sponsored by:
Vertiv
1050 Dearborn Dr.
Columbus, OH 43085

Evaluation Personnel:
Kenneth Lasoski
Joshua Gola
Acumen Security
2400 Research Blvd, Suite 395
Rockville, MD 20850

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
1.0	8/9/2021	Initial release
1.1	4/11/2022	Addressed NIAP comments
1.2	5/25/2022	Addressed NIAP comments
1.3	5/28/2022	Addressed NIAP comments
1.4	6/1/2022	Addressed NIAP comments

Contents

1 TOE Overview 12
2 Assurance Activities Identification 13
3 Test Equivalency Justification 14
3.1 Architectural Description 14
3.2 Hardware and Firmware Analysis 14
3.3 Specification of Differences 14
3.4 Equivalency Analysis 15
3.4.1 Base PP destructive testing 16
3.4.2 Platform/Hardware Dependencies 16
3.4.3 Differences in Libraries Used to Provide TOE Functionality 17
3.4.4 TOE Management Interface Differences 17
3.4.5 Tamper evidence equivalency 17
3.4.6 TOE Functional Differences 17
3.5 Recommendations/Conclusions 17
4 Test Bed Descriptions 26
4.1 Test Bed # 1 26
4.1.1 Visual Diagram 26
Diagram of the TOE, with how to connect cables and required equipment. 26
4.1.2 Test Equipment 26
4.1.3 Test Time & Location 28
4.1.4 Test Environment 29
4.1.5 Configuration Information 29
5 Detailed Test Cases (TSS, Isolation Document, and Guidance Activities) 30
5.1 TSS, Isolation Document, and Guidance Activities (Auditing) 30
5.1.1 FAU_GEN.1 30
5.1.1.1 FAU_GEN.1 Isolation Document 1 30
5.1.1.2 FAU_GEN.1 TSS 1 30
5.1.1.3 FAU_GEN.1 Guidance 1 31
5.2 TSS, Isolation Document, and Guidance Activities (User Data Protection) 31
5.2.1 FDP_AFL_EXT.1 31
5.2.1.1 FDP_AFL_EXT.1 Isolation Document 1 31
5.2.1.2 FDP_AFL.1 TSS 1 32
5.2.1.3 FDP_AFL.1 Guidance 1 32
5.2.2 FDP_APC_EXT.1 32
5.2.2.1 FDP_APC_EXT.1 Isolation Document 1 32
5.2.2.2 FDP_APC_EXT.1 TSS 1 32
5.2.2.3 FDP_APC_EXT.1 Guidance 1 33
5.2.3 FDP_APC_EXT.1/AO 33
5.2.3.1 FDP_APC_EXT.1/AO Isolation Document 1 33
5.2.3.2 FDP_APC_EXT.1/AO Isolation Document 2 33
5.2.3.3 FDP_APC_EXT.1/AO Isolation Document 3 34
5.2.3.4 FDP_APC_EXT.1/AO TSS 1 34
5.2.3.5 FDP_APC_EXT.1/AO Guidance 1 34

5.2.4 FDP_APC_EXT.1/KM 35
5.2.4.1 FDP_APC_EXT.1/KM Isolation Document 1 35
5.2.4.2 FDP_APC_EXT.1/KM TSS 1 35
5.2.4.3 FDP_APC_EXT.1/KM Guidance 1 35
5.2.5 FDP_APC_EXT.1/UA 35
5.2.5.1 FDP_APC_EXT.1/UA Isolation Document 1 35
5.2.5.2 FDP_APC_EXT.1/UA TSS 1 36
5.2.5.3 FDP_APC_EXT.1/UA Guidance 1 36
5.2.6 FDP_APC_EXT.1/VI 36
5.2.6.1 FDP_APC_EXT.1/VI Isolation Document 1 36
5.2.6.2 FDP_APC_EXT.1/VI TSS 1 36
5.2.6.3 FDP_APC_EXT.1/VI Guidance 1 36
5.2.7 FDP_CDS_EXT.1(1) 37
5.2.7.1 FDP_CDS_EXT.1(1) Isolation Document 1 37
5.2.7.2 FDP_CDS_EXT.1(1) TSS 1 37
5.2.7.3 FDP_CDS_EXT.1(1) Guidance 1 37
5.2.8 FDP_CDS_EXT.1(2) 37
5.2.8.1 FDP_CDS_EXT.1(2) Isolation Document 1 37
5.2.8.2 FDP_CDS_EXT.1(2) TSS 1 38
5.2.8.3 FDP_CDS_EXT.1(2) Guidance 1 38
5.2.9 FDP_FIL_EXT.1/KM 38
5.2.9.1 FDP_FIL_EXT.1/KM Isolation Document 1 38
5.2.9.2 FDP_FIL_EXT.1/KM TSS 1 38
5.2.9.3 FDP_FIL_EXT.1/KM Guidance 1 39
5.2.10 FDP_FIL_EXT.1/UA 39
5.2.10.1 FDP_FIL_EXT.1/UA Isolation Document 1 39
5.2.10.2 FDP_FIL_EXT.1/UA TSS 1 39
5.2.10.3 FDP_FIL_EXT.1/UA Guidance 1 39
5.2.11 FDP_IPC_EXT.1 40
5.2.11.1 FDP_IPC_EXT.1 Isolation Document 1 40
5.2.11.2 FDP_IPC_EXT.1 TSS 1 40
5.2.11.3 FDP_IPC_EXT.1 Guidance 1 40
5.2.12 FDP_PDC_EXT.1 40
5.2.12.1 FDP_PDC_EXT.1 Isolation Document 1 40
5.2.12.2 FDP_PDC_EXT.1 TSS 1 41
5.2.12.3 FDP_PDC_EXT.1 TSS 2 41
5.2.12.4 FDP_PDC_EXT.1 TSS 3 41
5.2.12.5 FDP_PDC_EXT.1 TSS 4 42
5.2.12.6 FDP_PDC_EXT.1 Guidance 1 42
5.2.12.7 FDP_PDC_EXT.1 Guidance 2 42
5.2.12.8 FDP_PDC_EXT.1 Guidance 3 43
5.2.12.9 FDP_PDC_EXT.1 Guidance 4 43
5.2.12.10 FDP_PDC_EXT.1 Guidance 1-KM, UA, VI 43
5.2.13 FDP_PDC_EXT.2/AO 43
5.2.13.1 FDP_PDC_EXT.2/AO Isolation Document 1 43
5.2.13.2 FDP_PDC_EXT.2/AO TSS 1 44
5.2.13.3 FDP_PDC_EXT.2/AO Guidance 1 44
5.2.14 FDP_PDC_EXT.2/KM 44
5.2.14.1 FDP_PDC_EXT.2/KM Isolation Document 1 44

5.2.14.2 FDP_PDC_EXT.2/KM TSS 1 44
5.2.14.3 FDP_PDC_EXT.2/KM Guidance 1 44
5.2.15 FDP_PDC_EXT.2/UA 44
5.2.16 FDP_PDC_EXT.2/VI 45
5.2.16.1 FDP_PDC_EXT.2/VI Isolation Document 1 45
5.2.16.2 FDP_PDC_EXT.2/VI TSS 1 45
5.2.16.3 FDP_PDC_EXT.2/VI Guidance 1 45
5.2.17 FDP_PDC_EXT.3/KM 45
5.2.17.1 FDP_PDC_EXT.3/KM Isolation Document 1 45
5.2.17.2 FDP_PDC_EXT.3/KM TSS 1 45
5.2.17.3 FDP_PDC_EXT.3/KM TSS 2 46
5.2.17.4 FDP_PDC_EXT.3/KM Guidance 1 46
5.2.18 FDP_PDC_EXT.3/VI 46
5.2.18.1 FDP_PDC_EXT.3/VI Isolation Document 1 46
5.2.18.2 FDP_PDC_EXT.3/VI TSS 1 46
5.2.18.3 FDP_PDC_EXT.3/VI Guidance 1 46
5.2.19 FDP_PDC_EXT.4 47
5.2.19.1 FDP_PDC_EXT.4 Isolation Document 1 47
5.2.19.2 FDP_PDC_EXT.4 TSS 1 47
5.2.19.3 FDP_PDC_EXT.4 TSS 2 47
5.2.19.4 FDP_PDC_EXT.4 Guidance 1 47
5.2.20 FDP_PUD_EXT.1 47
5.2.20.1 FDP_PUD_EXT.1 Isolation Document 1 47
5.2.20.2 FDP_PUD_EXT.1 TSS 1 48
5.2.20.3 FDP_PUD_EXT.1 TSS 2 48
5.2.20.4 FDP_PUD_EXT.1 Guidance 1 48
5.2.21 FDP_PWR_EXT.1 48
5.2.21.1 FDP_PWR_EXT.1 Isolation Document 1 48
5.2.21.2 FDP_PWR_EXT.1 TSS 1 49
5.2.21.3 FDP_PWR_EXT.1 Guidance 1 49
5.2.22 FDP_RDR_EXT.1 49
5.2.22.1 FDP_RDR_EXT.1 Isolation Document 1 49
5.2.22.2 FDP_RDR_EXT.1 TSS 1 49
5.2.22.3 FDP_RDR_EXT.1 Guidance 1 50
5.2.23 FDP_RIP_EXT.1 50
5.2.23.1 FDP_RIP_EXT.1 Isolation Document 1 50
5.2.23.2 FDP_RIP_EXT.1 TSS 1 50
5.2.23.3 FDP_RIP_EXT.1 TSS 2 50
5.2.23.4 FDP_RIP_EXT.1 Guidance 1 51
5.2.24 FDP_RIP.1/KM 51
5.2.24.1 FDP_RIP.1/KM Isolation Document 1 51
5.2.24.2 FDP_RIP.1/KM TSS 1 51
5.2.24.3 FDP_RIP.1/KM TSS 2 51
5.2.24.4 FDP_RIP.1/KM Guidance 1 52
5.2.25 FDP_RIP_EXT.2 52
5.2.25.1 FDP_RIP_EXT.2 Isolation Document 1 52
5.2.25.2 FDP_RIP_EXT.2 TSS 1 52
5.2.25.3 FDP_RIP_EXT.2 TSS 2 53
5.2.25.4 FDP_RIP_EXT.2 Guidance 1 53

5.2.26 FDP_SPR_EXT.1/DP 53
5.2.26.1 FDP_SPR_EXT.1/DP Isolation Document 1 53
5.2.26.2 FDP_SPR_EXT.1/DP TSS 1 53
5.2.26.3 FDP_SPR_EXT.1/DP Guidance 1 54
5.2.27 FDP_SPR_EXT.1/HDMI 54
5.2.27.1 FDP_SPR_EXT.1/HDMI Isolation Document 1 54
5.2.27.2 FDP_SPR_EXT.1/HDMI TSS 1 54
5.2.27.3 FDP_SPR_EXT.1/HDMI Guidance 1 54
5.2.28 FDP_SPR_EXT.1/USB 54
5.2.28.1 FDP_SPR_EXT.1/USB Isolation Document 1 54
5.2.28.2 FDP_SPR_EXT.1/USB TSS 1 54
5.2.28.3 FDP_SPR_EXT.1/USB Guidance 1 55
5.2.29 FDP_SWI_EXT.1 55
5.2.29.1 FDP_SWI_EXT.1 Isolation Document 1 55
5.2.29.2 FDP_SWI_EXT.1 TSS 1 55
5.2.29.3 FDP_SWI_EXT.1 TSS 2 55
5.2.29.4 FDP_SWI_EXT.1 Guidance 1 56
5.2.30 FDP_SWI_EXT.2(1) 56
5.2.30.1 FDP_SWI_EXT.2(1) Isolation Document 1 56
5.2.30.2 FDP_SWI_EXT.2(1) TSS 1 56
5.2.30.3 FDP_SWI_EXT.2(1) Guidance 1 57
5.2.31 FDP_SWI_EXT.2(2) 57
5.2.31.1 FDP_SWI_EXT.2(2) Isolation Document 1 57
5.2.31.2 FDP_SWI_EXT.2(2) TSS 1 57
5.2.31.3 FDP_SWI_EXT.2(2) Guidance 1 57
5.2.32 FDP_SWI_EXT.3 58
5.2.32.1 FDP_SWI_EXT.3 Isolation Document 1 58
5.2.32.2 FDP_SWI_EXT.3 TSS 1 58
5.2.32.3 FDP_SWI_EXT.3 Guidance 1 58
5.2.33 FDP_TER_EXT.1 59
5.2.33.1 FDP_TER_EXT.1 Isolation Document 1 59
5.2.33.2 FDP_TER_EXT.1 TSS 1 59
5.2.33.3 FDP_TER_EXT.1 Guidance 1 59
5.2.34 FDP_TER_EXT.2 59
5.2.34.1 FDP_TER_EXT.2 Isolation Document 1 59
5.2.34.2 FDP_TER_EXT.2 TSS 1 60
5.2.34.3 FDP_TER_EXT.2 Guidance 1 60
5.2.35 FDP_TER_EXT.3 60
5.2.35.1 FDP_TER_EXT.3 Isolation Document 1 60
5.2.35.2 FDP_TER_EXT.3 TSS 1 60
5.2.35.3 FDP_TER_EXT.3 Guidance 1 61
5.2.36 FDP_UAI_EXT.1 61
5.2.36.1 FDP_UAI_EXT.1 Isolation Document 1 61
5.2.36.2 FDP_UAI_EXT.1 TSS 1 61
5.2.36.3 FDP_UAI_EXT.1 Guidance 1 62
5.2.37 FDP_UDF_EXT.1/AO 62
5.2.37.1 FDP_UDF_EXT.1/AO Isolation Document 1 62
5.2.37.2 FDP_UDF_EXT.1/AO TSS 1 62
5.2.37.3 FDP_UDF_EXT.1/AO Guidance 1 62

5.2.38 FDP_UDF_EXT.1/KM 63
5.2.38.1 FDP_UDF_EXT.1/KM Isolation Document 1 63
5.2.38.2 FDP_UDF_EXT.1/KM TSS 1 63
5.2.38.3 FDP_UDF_EXT.1/KM TSS 2 63
5.2.38.4 FDP_UDF_EXT.1/KM Guidance 1 63
5.2.39 FDP_UDF_EXT.1/VI 64
5.2.39.1 FDP_UDF_EXT.1/VI Isolation Document 1 64
5.2.39.2 FDP_UDF_EXT.1/VI TSS 1 64
5.2.39.3 FDP_UDF_EXT.1/VI Guidance 1 64
5.3 TSS, Isolation Document, and Guidance Activities (Identification and Authentication) 64
5.3.1 FIA_UAU.2 64
5.3.2 FIA_UID.2 64
5.4 TSS, Isolation Document, and Guidance Activities (Security Management) 64
5.4.1 FMT_MOF.1 64
5.4.1.1 FMT_MOF.1 Isolation Document 1 64
5.4.1.2 FMT_MOF.1 TSS 1 65
5.4.1.3 FMT_MOF.1 TSS 2 65
5.4.1.4 FMT_MOF.1 TSS 3 65
5.4.1.5 FMT_MOF.1 Guidance 1 66
5.4.2 FMT_SMF.1 66
5.4.2.1 FMT_SMF.1 Isolation Document 1 66
5.4.2.2 FMT_SMF.1 TSS 1 66
5.4.2.3 FMT_SMF.1 Guidance 1 67
5.4.3 FMT_SMR.1 67
5.5 TSS, Isolation Document, and Guidance Activities (Protection of the TSF) 67
5.5.1 FPT_FLS_EXT.1(1) 67
5.5.2 FPT_FLS_EXT.1(2) 67
5.5.3 FPT_NTA_EXT.1 67
5.5.3.1 FPT_NTA_EXT.1 Isolation Document 1 67
5.5.3.2 FPT_NTA_EXT.1 TSS 1 68
5.5.3.3 FPT_NTA_EXT.1 Guidance 1 68
5.5.4 FPT_PHP.1 68
5.5.4.1 FPT_PHP.1 Isolation Document 1 68
5.5.4.2 FPT_PHP.1 TSS 1 69
5.5.4.3 FPT_PHP.1 Guidance 1 69
5.5.5 FPT_PHP.3 69
5.5.5.1 FPT_PHP.3 Isolation Document 1 69
5.5.5.2 FPT_PHP.3 TSS 1 69
5.5.5.3 FPT_PHP.3 Guidance 1 70
5.5.5.4 FPT_PHP.3 Guidance 2 70
5.5.6 FPT_STM.1 70
5.5.6.1 FPT_STM.1 Isolation Document 1 70
5.5.6.2 FPT_STM.1 TSS 1 71
5.5.6.3 FPT_STM.1 Guidance 1 71
5.5.7 FPT_TST.1(1) 71
5.5.7.1 FPT_TST.1(1) Isolation Document 1 71
5.5.7.2 FPT_TST.1(1) TSS 1 71

5.5.7.3 FPT_TST.1(1) TSS 2 72
5.5.7.4 FPT_TST.1(1) TSS 3 72
5.5.7.5 FPT_TST.1(1) TSS 4 72
5.5.7.6 FPT_TST.1(1) Guidance 1 73
5.5.8 FPT_TST.1(2) 73
5.5.8.1 FPT_TST.1(2) Isolation Document 1 73
5.5.8.2 FPT_TST.1(2) TSS 1 73
5.5.8.3 FPT_TST.1(2) TSS 2 74
5.5.8.4 FPT_TST.1(2) TSS 3 74
5.5.8.5 FPT_TST.1(2) TSS 4 74
5.5.8.6 FPT_TST.1(2) Guidance 1 75
5.5.9 FPT_TST_EXT.1 75
5.5.9.1 FPT_TST_EXT.1 Isolation Document 1 75
5.5.9.2 FPT_TST_EXT.1 TSS 1 75
5.5.9.3 FPT_TST_EXT.1 Guidance 1 75
5.5.9.4 FPT_TST_EXT.1 Guidance 2 76
5.6 TSS, Isolation Document, and Guidance Activities (TOE Access) 76
5.6.1 FTA_CIN_EXT.1 76
5.6.1.1 FTA_CIN_EXT.1 Isolation Document 1 76
5.6.1.2 FTA_CIN_EXT.1 TSS 1 76
5.6.1.3 FTA_CIN_EXT.1 TSS 2 76
5.6.1.4 FTA_CIN_EXT.1 Guidance 1 77
5.6.1.5 FTA_CIN_EXT.1 Guidance 2 77
6 Detailed Test Cases (Test Activities) 78
6.1 FAU_GEN.1 Test 1 78
6.2 FDP_AFL_EXT.1 Test 1 81
6.3 FDP_APC_EXT.1 Test 1 82
6.4 FDP_APC_EXT.1/AO Test 1 83
6.5 FDP_APC_EXT.1/AO Test 2 85
6.6 FDP_APC_EXT.1/AO Test 3 88
6.7 FDP_APC_EXT.1/AO Test 4 91
6.8 FDP_APC_EXT.1/KM Test 1 92
6.9 FDP_APC_EXT.1/KM Test 2 95
6.10 FDP_APC_EXT.1/KM Test 3 98
6.11 FDP_APC_EXT.1/KM Test 4 101
6.12 FDP_APC_EXT.1/KM Test 5 102
6.13 FDP_APC_EXT.1/UA Test 1 104
6.14 FDP_APC_EXT.1/UA Test 2 106
6.15 FDP_APC_EXT.1/UA Test 3 109
6.16 FDP_APC_EXT.1/UA Test 4 110
6.17 FDP_APC_EXT.1/VI Test 1 111
6.18 FDP_APC_EXT.1/VI Test 2 113
6.19 FDP_APC_EXT.1/VI Test 3 116
6.20 FDP_APC_EXT.1/VI Test 4 120
6.21 FDP_APC_EXT.1/VI Test 5 122
6.22 FDP_CDS_EXT.1(1) Test 1 124
6.23 FDP_CDS_EXT.1(2) Test 1 124

6.24 FDP_FIL_EXT.1/KM Test 1 124
6.25 FDP_FIL_EXT.1/KM Test 2 125
6.26 FDP_FIL_EXT.1/UA Test 1 126
6.27 FDP_FIL_EXT.1/UA Test 2 126
6.28 FDP_FIL_EXT.1/UA Test 3 127
6.29 FDP_IPC_EXT.1 Test 1 128
6.30 FDP_PDC_EXT.1 Test 1 128
6.31 FDP_PDC_EXT.1 Test 2 128
6.32 FDP_PDC_EXT.1 Test 3 129
6.33 FDP_PDC_EXT.1 Test 1-AO 131
6.34 FDP_PDC_EXT.1 Test 1-KM 132
6.35 FDP_PDC_EXT.1 Test 2-KM 134
6.36 FDP_PDC_EXT.1 Test 1-UA 135
6.37 FDP_PDC_EXT.1 Test 2-UA 137
6.38 FDP_PDC_EXT.1 Test 1-VI 138
6.39 FDP_PDC_EXT.2/AO Test 1 139
6.40 FDP_PDC_EXT.2/KM Test 1 140
6.41 FDP_PDC_EXT.2/VI Test 1 141
6.42 FDP_PDC_EXT.3/KM Test 1 141
6.43 FDP_PDC_EXT.2/UA Test 1 141
6.44 FDP_PDC_EXT.3/VI Test 1 141
6.45 FDP_PDC_EXT.4 Test 1 141
6.46 FDP_PUD_EXT.1 Test 1 141
6.47 FDP_PWR_EXT.1 Test 1 143
6.48 FDP_RDR_EXT.1 Test 1 143
6.49 FDP_RIP_EXT.1 Test 1 145
6.50 FDP_RIP.1/KM Test 1 145
6.51 FDP_RIP_EXT.2 Test 1 145
6.52 FDP_SPR_EXT.1/DP Test 1 146
6.53 FDP_SPR_EXT.1/HDMI Test 1 146
6.54 FDP_SPR_EXT.1/USB Test 1 146
6.55 FDP_SWI_EXT.1 Test 1 146
6.56 FDP_SWI_EXT.2(1) Test 1 146
6.57 FDP_SWI_EXT.2(2) Test 1 146
6.58 FDP_SWI_EXT.3 Test 1 147
6.59 FDP_TER_EXT.1 Test 1 147
6.60 FDP_TER_EXT.2 Test 1 147
6.61 FDP_TER_EXT.3 Test 1 147
6.62 FDP_UAI_EXT.1 Test 1 147
6.63 FDP_UAI_EXT.1 Test 2 149
6.64 FDP_UAI_EXT.1 Test 3 150
6.65 FDP_UDF_EXT.1/AO Test 1 150
6.66 FDP_UDF_EXT.1/KM Test 1 152
6.67 FDP_UDF_EXT.1/VI Test 1 152
6.68 FMT_MOF.1 Test 1 152
6.69 FMT_SMF.1 Test 1 153

6.70 FPT_NTA_EXT.1 Test 1 154
6.71 FPT_PHP.1 Test 1 154
6.72 FPT_PHP.1 Test 2 155
6.73 FPT_PHP.3 Test 1 155
6.74 FPT_STM.1 Test 1 157
6.75 FPT_TST.1(1) and FPT_TST.1(2) Test 1 157
6.76 FPT_TST_EXT.1 Test 1 158
6.77 FTA_CIN_EXT.1 Test 1 159
7 Security Assurance Requirements 162
7.1 ADV_FSP.1 Basic Functional Specification 162
7.1.1 ADV_FSP.1 162
7.1.1.1 ADV_FSP.1 Activity 1 162
7.2 AGD_OPE.1 Operational User Guidance 162
7.2.1 AGD_OPE.1 162
7.2.1.1 AGD_OPE.1 Activity 1 162
7.3 AGD_PRE.1 Preparative Procedures 162
7.3.1 AGD_PRE.1 162
7.3.1.1 AGD_PRE.1 Activity 1 162
7.4 ALC Assurance Activities 163
7.4.1 ALC_CMC.1 163
7.4.1.1 ALC_CMC.1 Activity 1 163
7.4.2 ALC_CMS.1 163
7.4.2.1 ALC_CMS.1 Activity 1 163
7.5 ATE_IND.1 Independent Testing – Conformance 163
7.5.1 ATE_IND.1 163
7.5.1.1 ATE_IND.1 Activity 1 163
7.6 AVA_VAN.1 Vulnerability Survey 164
7.6.1 AVA_VAN.1 164
7.6.1.1 AVA_VAN.1 Activity 1 164
8 Conclusion 166
9 Evaluation Evidence 167
10 References 168

1 TOE Overview

The Vertiv Secure Peripheral Sharing Devices (PSD) allow users to share keyboard, video, and mouse peripherals between a number of connected computers. The devices also allow for the sharing of audio and Universal Serial Bus (USB) authentication device peripherals.

The following security features are provided by the Vertiv Peripheral Sharing Devices:

- Video Security
    - Computer video input interfaces are isolated through the use of separate electronic components, power and ground domains
    - The display is isolated by dedicated, read-only, Extended Display Identification Data (EDID) emulation for each computer
    - Access to the monitor's EDID is blocked
    - Access to the Monitor Control Command Set (MCCS commands) is blocked
    - Both DisplayPort and High-Definition Multimedia Interface (HDMI) video peripherals are supported on the SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM145DPH, SCM185DPH, SC985DPH and SCMV285DPH devices
    - Video input is accepted as DisplayPort or HDMI on all devices, and as USB-Type C with DisplayPort as an alternate function on the SC845DPHC and SC945DPHC devices
- Keyboard and Mouse Security
    - The keyboard and mouse are isolated by dedicated, USB device emulation for each computer
    - One-way, peripheral-to-computer data flow is enforced through unidirectional optical data diodes
    - Communication from computer-to-keyboard/mouse is blocked
    - Non HID (Human Interface Device) data transactions are blocked
- Authentication Device
    - Unauthorized USB devices are blocked
    - USB authentication devices are authorized by default; all other devices are blocked by default
    - Devices may be whitelisted or blacklisted based on Vendor Identification/Product Identification (VID/PID) characteristics
    - Secure management functions allow configuration of allowed devices, and maintain a record of any changes to that configuration
- Audio Security
    - One-way computer to speaker sound flow is enforced through unidirectional optical data diodes
- Hardware Anti-Tampering
    - On the SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM145DPH, SCM185DPH, SC985DPH devices, any attempt to open the product enclosure will activate an anti-tampering system, making the product inoperable and indicating tampering via blinking Light Emitting Diodes (LEDs)
    - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised

2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the Protection Profile for Peripheral Sharing Device, Version: 4.0 and the following PP modules:

- PP-Module for Analog Audio Output Devices, Version 1.0
- PP-Module for User Authentication Devices, Version 1.0
- PP-Module for Keyboard/Mouse Devices, Version 1.0
- PP-Module for Video/Display Devices, Version 1.0

SRFs have been selected in accordance with PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, 19 July 2019 and on the selections within the PP and modules.

3 Test Equivalency Justification

3.1 Architectural Description

The Vertiv Secure Keyboard, Video, Mouse (KVM) Switches allow users to share keyboard, video, and mouse peripherals between a number of connected computers. These devices also allow for the sharing of audio and Universal Serial Bus (USB) authentication device peripherals.

The Vertiv Secure Matrix Switches allow users to view and control two computers while securely sharing keyboard, video, mouse, and audio peripherals between a number of connected computers. These TOE devices also allow for the sharing of USB authentication device peripherals.

The Vertiv Secure Combiner Switches allow users to interact with multiple computers presented on the same displays at the same time using a single set of keyboard, mouse, and video peripherals. This device also allows for the sharing of audio and USB authentication device peripherals.

The models being included are listed in Section 3.3 and 3.5.

3.2 Hardware and Firmware Analysis

These devices use the same system controller board, video boards and firmware. They do not contain Central Processing Units (CPU) but instead function using 32-bit microcontrollers from STMicroelectronics. There are slight variances of microcontrollers used, but they are all 32-bit STMicroelectronics brand and as such use the same instructions.

3.3 Specification of Differences

The following table provides a breakdown of the physical differences between hardware models. All models have Tamper Evident Labels, support user authentication and audit logging, keyboard and mouse, analog audio and user authentication device peripherals.

Family	Family Description	Part Number	Model	Active Anti-tampering	Tamper Evident labels	User Authentication and audit logging	Analog Audio	Video in	Video out	Number of supported displays	KM	Authentication Device Peripheral (DPP)
KVM	KVM devices with Active Anti-tampering, Analog Audio, User authentication (Dedicated Peripheral Port (DPP)) and audit logging.	CGA19205	SC845DPH	Yes	Yes	Yes	Yes	DP/HDMI	DP/HDMI	1	Yes	Yes
		CGA19206	SC945DPH	Yes	Yes	Yes	Yes	DP/HDMI	DP/HDMI	2	Yes	Yes
		CGA20363	SC845DPHC	Yes	Yes	Yes	Yes	DP/HDMI+ USB Type C	DP/HDMI	1	Yes	Yes
		CGA20365	SC945DPHC	Yes	Yes	Yes	Yes	DP/HDMI+ USB Type C	DP/HDMI	2	Yes	Yes
		CGA19215	SC985DPH	Yes	Yes	Yes	Yes	DP/HDMI	DP/HDMI	2	Yes	Yes
Matrix	KVM Matrix devices with Active Anti-tampering, Analog Audio, User authentication (Dedicated Peripheral Port (DPP)) and audit logging.	CGA18676	SCM145DPH	Yes	Yes	Yes	Yes	DP/HDMI	DP/HDMI	2	Yes	Yes
		CGA18678	SCM185DPH	Yes	Yes	Yes	Yes	DP/HDMI	DP/HDMI	2	Yes	Yes
Combiner	Secure KVM Combiner with audio, User authentication and audit logging.	CGA18687	SCMV245DPH	No	Yes	Yes	Yes	DP/HDMI	HDMI	2	Yes	Yes
		CGA18697	SCMV285DPH	No	Yes	Yes	Yes	DP/HDMI	DP/HDMI	2	Yes	Yes

Table 1 – Device Differences

3.4 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 [PP].

The following tables provide a comparison of the model equivalency groupings. Those proposed for testing are shown in **bold**.

Model	System Controller PCBA	System Cont. firmware	Video Cont. firmware	Video Input	Video Output	Product Description	Device Group per ST
SC845DPH	Same	Same	Same	DP/HDMI	DP/HDMI	CYBEX™ SC Universal DP/H Secure KVM Switch 4-Port Single Display with CAC	A
SC945DPH				DP/HDMI	DP/HDMI	CYBEX™ SC Universal DP/H Secure KVM Switch 4-Port Dual Display with CAC **Used for Base PP testing only**	B
SCM145DPH				DP/HDMI	DP/HDMI	CYBEX™ SC Universal DP/H Secure Desktop Matrix 2x4 KVM with CAC	B
SCM185DPH				**DP/HDMI**	**DP/HDMI**	**CYBEX™ SC Universal DP/H Secure Desktop Matrix 2x8 KVM with CAC**	B
SC985DPH				DP/HDMI	DP/HDMI	CYBEX™ SC Universal DP/H Secure KVM Switch 8-Port Dual Display with CAC	B

Table 2 - Secure KVM and KVM Matrix models with Active Anti-tampering, Analog Audio, User Authentication, Dedicated Peripheral Port and audit logging with the same Video Input/Output ports (DP/HDMI).

Model	System Controller PCBA	System Cont. firmware	Video Cont. firmware	Video Input	Video Output	Product Description	Device Group per ST
SC845DPHC	Same	Same	Same	**DP/HDMI /USB C**	**DP/HDMI**	**CYBEX™ SC Universal DPH + USB-C secure KVM Switch 4-Port Single Display w/CAC**	C

Model	System Controller PCBA	System Cont. firmware	Video Cont. firmware	Video Input	Video Output	Product Description	Device Group per ST
SC945DPHC				DP/HDMI /USB C	DP/HDMI	CYBEX™ SC Universal DPH + USB-C secure KVM Switch 4-Port dual Display w/CAC	E

Table 3 - Secure KVM models with Active Anti-tampering, Analog Audio, User Authentication, Dedicated Peripheral Port and audit logging with the same Video Input/Output ports (DP/HDMI/USB Type C).

Model	System Controller PCBA	System Cont. firmware	Video Cont. firmware	Video Input	Video Output	Product Description	Product Group per ST
SCMV245DPH	Same	Same	Same	DP/HDMI	HDMI	CYBEX™ SC Universal DP/H Secure 4-Port MultiViewer KVM with CAC	F
SCMV285DPH				DP/HDMI	DP/HDMI	CYBEX™ SC Universal DP/H Secure 8-Port MultiViewer KVM with CAC	D

Table 4 - Secure KVM Combiner models with Audio, User Authentication with the same Video Input/Output ports (DP/HDMI).

3.4.1 Base PP destructive testing

The lab has selected three units to perform all testing on (SCM185DPH, SC845DPHC, SCMV245DPH). This along with the equivalency rationale provides coverage for all KVM devices identified in the Security Target. As some testing requirements in the Base PP (Base PP Module for Peripheral Sharing Devices) are destructive in nature, it was decided to use a spare unit (SC945DPH) to perform these tests across devices and claim equivalency. As discussed later here the anti-tamper evidence seal and anti-tamper switch functionality are the same across all KVM units. The SC945DPH unit were rendered disabled from destructive testing. The destructive tests are FPT_PHP.1 Test 1 and Test 2, and FPT_PHP.3 Test 1.

3.4.2 Platform/Hardware Dependencies

All of the security functionality, with the exception of video is provided on the system controller board. The basic system controller boards vary by the number of supported ports. All of the 4 port products

share the same system controller board. Likewise, all of the 8 port products use the same system controller board. System controller boards do not operate any differently and support the exact same functionality independent of the number of output ports. The system controller boards for all products use the same firmware.

All video boards share the same firmware. All video boards with the same video input and video out combinations are the same. This is how all models are grouped above.

Dual head products include two instances of the same video board stacked on top of one another in the final assembly. The instances are isolated from each other to mitigate any security impact. The lab considers the number of externally supported monitors (1 or 2) to be equivalent as there is no difference in the way the KVMs operate.

Matrix products use the same video boards and firmware as the other products with the same number of ports. The difference is that an additional video output is assembled on the boards.

With respect to equivalency in testing of multiple KM, video and audio ports, each port is considered equivalent due to being driven by the exact same microcontroller and firmware thus are expected to behave functionally identical to each other. Throughout the course of testing, the evaluators used a sampling of port testing covering various permutations to ensure adequate coverage. These permutations are justified in each applicable test case within the test report. Each unique protocol (e.g. DVI and HDMI) is covered. To show sufficient testing coverage (assuming all ports are equivalent), a subset of port testing will be performed, specifically for conclusive steps of the test cases where the PP specifically asks to test all non-selected computers.

3.4.3 Differences in Libraries Used to Provide TOE Functionality

Firmware is the same for all models.

3.4.4 TOE Management Interface Differences

All devices support the same management interface, called terminal mode.

3.4.5 Tamper evidence equivalency

The tamper evident seal used across all the Vertiv units is the same, so the expected evidence will not be any different. All devices support tamper evident labels including the remote controls. Active Anti-tampering is supported on the KVM family but not on Combiners. The Anti-Tamper Switch used to detect physical breaches by Vertiv is the same across all units. The method of secret key erasure and unit disabling is also exactly the same.

The remote controls also support an Anti-Tamper Switch which is identical between remote control models.

3.4.6 TOE Functional Differences

Each hardware model within the TOE boundary provides identical SFR 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. Result: All platforms are functionally equivalent.

3.5 Recommendations/Conclusions

Based on the equivalency rationale listed above, testing was performed on each of the BOLD selections of hardware models in the table below. Devices from groups B, C, and F were selected. Coverage for SFR testing of devices in groups A, D, and E is already provided by testing of the SFR iterations of the ST, each of which apply to multiple device groups (i.e. Each SFR in the ST is mapped to a set of device groups. Each of these mappings includes at least one of the selected models for testing. Each assurance activity was performed with the appropriate conditions for each tested device.

Video Input	USB/Keyboard/Mouse	Model	Video Output	Product Description	Product Group
DP/HDMI	Same	SC845DPH	DP/HDMI	CYBEX™ SC Universal DP/H Secure KVM Switch 4-Port Single Display with CAC	A
DP/HDMI		**SC945DPH**	**DP/HDMI**	**CYBEX™ SC Universal DP/H Secure KVM Switch 4-Port Dual Display with CAC** **Used for Base PP testing only**	B
DP/HDMI		SCM145DPH	DP/HDMI	CYBEX™ SC Universal DP/H Secure Desktop Matrix 2x4 KVM with CAC	B
DP/HDMI		**SCM185DPH**	**DP/HDMI**	**CYBEX™ SC Universal DP/H Secure Desktop Matrix 2x8 KVM with CAC**	B
DP/HDMI		SC985DPH	DP/HDMI	CYBEX™ SC Universal DP/H Secure KVM Switch 8-Port Dual Display with CAC	B
DP/HDMI/USB C		**SC845DPHC**	**DP/HDMI**	**CYBEX™ SC Universal DPH + USB-C secure KVM Switch 4-Port Single Display w/CAC**	C
DP/HDMI/USB C		SC945DPHC	DP/HDMI	CYBEX™ SC Universal DPH + USB-C secure KVM Switch 4-Port dual Display w/CAC	E
DP/HDMI		**SCMV245DPH**	**HDMI**	**CYBEX™ SC Universal DP/H Secure 4-Port MultiViewer KVM with CAC**	F
DP/HDMI		SCMV285DPH	DP/HDMI	CYBEX™ SC Universal DP/H Secure 8-Port MultiViewer KVM with CAC	D

Table 5 – Tested Devices

Based on the equivalency rationale listed above, Base PP PSD v4.0 testing will be performed in full on the following hardware; SC945DPH, SCM185DPH, SC845DPHC, and SCMV245DPH. The three anti-tamper and active anti-tamper test cases will only be run on the SC945DPH.

All PP Module testing will be performed on the SC945DPH, SCM185DPH, SC845DPHC hardware units used in the equivalency rationale. Multi-display support will be tested using the SCM185DPH.

Test Case – **Base PP v4.0 – Peripheral Sharing Device**	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH	SFR/Rationale
FDP_PDC_EXT.1 - Test 1	X	X	X	X	FDP_PDC_EXT.1
FDP_PDC_EXT.1 - Test 2	X	X	X	X	FDP_PDC_EXT.1
FDP_PDC_EXT.1 - Test 3	X	X	X	X	FDP_PDC_EXT.1

FPT_PHP.1 - Test 1	X				FPT_PHP.1 - The KVM metal surface material upon which the labels are applied across all units' chassis are identical, thus the adhesion and tamper evidence characteristics are expected to be identical. This is a destructive tamper evident seal test. All units have the same tamper seal, so this test was run on one unit only.
FPT_PHP.1 - Test 2	X				FPT_PHP.1 - The KVM metal surface material upon which the labels are applied across all units' chassis are identical, thus the adhesion and tamper evidence characteristics are expected to be identical. This is a destructive tamper evident seal test. All units have the same tamper seal, so this test was run on one unit only.
FPT_TST.1(1) - Test 1	X	X	X		FPT_TST.1 - Active anti-tamper functionality
FPT_TST.1(2) - Test 1				X	FPT_TST.1
FPT_TST_EXT.1 – Test 1	X	X	X	X	FPT_TST_EXT.1
FAU_GEN.1 – Test 1	X	X	X	X	FAU_GEN.1
FMT_MOF.1 - Test 1	X	X	X	X	FMT_MOF.1
FMT_SMF.1 - Test 1	X	X	X	X	FMT_SMF.1
FPT_STM.1 - Test 1	X	X	X	X	FPT_STM.1
FDP_RIP_EXT.2 - Test 1	X	X	X	X	FDP_RIP_EXT.2
FPT_PHP.3 - Test 1	X				FPT_PHP.3 - This destructive test opens the unit and triggers the active anti-tamper switch, rendering the unit inoperable. All units use the same switch and erasure mechanism, so this test was run on one unit only. As multiple remotes are supported, the tamper evidence function is

					equivalent as all remotes are identical.
FTA_CIN_EXT.1 - Test 1	X	X	X	X	FTA_CIN_EXT.1

Test Case – **PP Module KM – Keyboard/Mouse**	SCM185DPH	SC845DPHC	SCMV245DPH	SFR/Rationale
FDP_APC_EXT - Test 1	X	X	X	FDP_APC_EXT.1/KM & FDP_SWI_EXT.2 Methodology includes testing ports #1 and #2, then move the test computers over to ports #3 and #4, then #5 and #6 (if applicable) and then #7 and #8. This ensures ports (#1, #2, #3, #4) or (#1, #2, #3, #4, #5, #6, #7, #8) were all tested. The evaluator confirms that cross testing between scenarios (Computers #1 and #2, Computers #3 and #4, Computers #5 and #6 and Computers #7 and #8 if applicable) were all completed so that a diverse sampling of testing occurred to cover overlaps between different computer selections.
FDP_APC_EXT - Test 2	X	X	X	FDP_APC_EXT.1/KM See above The evidence presented shows testing of all source ports in the relevant test steps and then a sampling of target port permutations as follows: • 4 port ○ (1-2) ○ (3-4) ○ (1-4) ○ (2-3) • 8 port ○ (1-2) ○ (3-4) ○ (5-6)

				○ (7-8)
FDP_APC_EXT - Test 3	X	X	X	FDP_APC_EXT.1/KM See above
FDP_APC_EXT - Test 4	X	X	X	FDP_APC_EXT.1/KM See above The evidence presented shows testing of all source ports in the relevant test steps and then a sampling of target port permutations as follows: • 4 port ○ (1-2) ○ (3-4) ○ (1-4) ○ (2-3) • 8 port ○ (1-2) ○ (3-4) ○ (5-6) ○ (7-8)
FDP_APC_EXT - Test 5	X	X	X	FDP_APC_EXT.1/KM See above
FDP_PDC_EXT - Test 1	X	X	X	FDP_PDC_EXT.2/KM & FDP_PDC_EXT.3/KM
FDP_PDC_EXT - Test 2	X	X	X	FDP_PDC_EXT.2/KM & FDP_PDC_EXT.3/KM
FDP_FIL_EXT - Test 1	X	X	X	FDP_FIL_EXT.1/KM
FDP_FIL_EXT - Test 2				Not selected / NA
FDP_RDR_EXT - Test 1	X	X	X	FDP_RDR_EXT

Test Case – **PP Module AO – Analog Audio Output**	SCM185DPH	SC845DPHC	SCMV245DPH	SFR/Rationale
FDP_APC_EXT - Test 1	X	X	X	FDP_APC_EXT.1/AO & FDP_SWI_EXT.2 Methodology includes testing ports #1 and #2, then move the test computers over to ports #3 and #4, then #5 and #6 (if applicable) and then #7 and #8. This ensures ports (#1, #2, #3, #4) or (#1, #2, #3, #4, #5, #6, #7, #8) were all tested. The evaluator confirms that cross testing

				between scenarios (Computers #1 and #2, Computers #3 and #4, Computers #5 and #6 and Computers #7 and #8 if applicable) were all completed so that a diverse sampling of testing occurred to cover overlaps between different computer selections.
FDP_APC_EXT - Test 2	X	X	X	FDP_APC_EXT.1/AO See above The evidence presented shows testing of all source ports in the relevant test steps and then a sampling of target port permutations as follows: • 4 port ○ (1-2) ○ (3-4) ○ (1-4) ○ (2-3) • 8 port ○ (1-2) ○ (3-4) ○ (5-6) ○ (7-8)
FDP_APC_EXT - Test 3	X	X	X	FDP_APC_EXT.1/AO See above
FDP_APC_EXT - Test 4	X	X	X	FDP_APC_EXT.1/AO See above
FDP_AFL_EXT - Test 1	X	X	X	FDP_AFL_EXT.1
FDP_PDC_EXT - Test 1	X	X	X	FDP_PDC_EXT.2/AO
FDP_PDC_EXT - Test 2	X	X	X	FDP_PDC_EXT.2/AO
FDP_PUD_EXT - Test 1	X	X	X	FDP_PUD_EXT.1
FDP_UDF_EXT - Test 1	X	X	X	FDP_UDF_EXT.1/AO

Test Case – **PP Module VI – Video Display**	SCM185DPH	SC845DPHC	SCMV245DPH	SFR/Rationale
FDP_APC_EXT - Test 1	X	X	X	FDP_APC_EXT.1/VI – Single display support as per FDP_CDS_EXT.1(2). Multi-display support was also tested on

				SCM185DPH as per FDP_CDS_EXT.1(1) Methodology includes testing ports #1 and #2, then move the test computers over to ports #3 and #4, then #5 and #6 (if applicable) and then #7 and #8. This ensures ports (#1, #2, #3, #4) or (#1, #2, #3, #4, #5, #6, #7, #8) were all tested. The evaluator confirms that cross testing between scenarios (Computers #1 and #2, Computers #3 and #4, Computers #5 and #6 and Computers #7 and #8 if applicable) were all completed so that a diverse sampling of testing occurred to cover overlaps between different computer selections.

FDP_APC_EXT - Test 2	X	X	X	FDP_APC_EXT.1/VI – Single display support as per FDP_CDS_EXT.1(2). Multi-display support was also tested on SCM185DPH as per FDP_CDS_EXT.1(1)
				
				See above
				
				The evidence presented shows testing of all source ports in the relevant test steps and then a sampling of target port permutations as follows:
				
				• 4 port
				  ○ (1-2)
				  ○ (3-4)
				  ○ (1-4)
				  ○ (2-3)
				• 8 port

				○ (1-2) ○ (3-4) ○ (5-6) ○ (7-8)
FDP_APC_EXT - Test 3	X	X	X	FDP_APC_EXT.1/VI
FDP_APC_EXT - Test 4	X	X	X	FDP_APC_EXT.1/VI
FDP_APC_EXT - Test 5	X	X	X	FDP_APC_EXT.1/VI
FDP_PDC_EXT - Test 1	X	X	X	FDP_PDC_EXT.2/VI & FDP_PDC_EXT.3/VI

Test Case – **PP Module UA – User Authentication**	SCM185DPH	SC845DPHC	SCMV245DPH	SFR/Rationale
FDP_APC_EXT - Test 1	X	X	X	FDP_APC_EXT.1/UA & FDP_SWI_EXT.2 Methodology includes testing ports #1 and #2, then move the test computers over to ports #3 and #4, then #5 and #6 (if applicable) and then #7 and #8. This ensures ports (#1, #2, #3, #4) or (#1, #2, #3, #4, #5, #6, #7, #8) were all tested. The evaluator confirms that cross testing between scenarios (Computers #1 and #2, Computers #3 and #4, Computers #5 and #6 and Computers #7 and #8 if applicable) were all completed so that a diverse sampling of testing occurred to cover overlaps between different computer selections.
FDP_APC_EXT - Test 2	X	X	X	FDP_APC_EXT.1/UA See above
FDP_APC_EXT - Test 3	X	X	X	FDP_APC_EXT.1/UA See above
FDP_APC_EXT - Test 4	X	X	X	FDP_APC_EXT.1/UA See above
FDP_PDC_EXT - Test 1	X	X	X	FDP_PDC_EXT.2/UA
FDP_PDC_EXT - Test 2	X	X	X	FDP_PDC_EXT.2/UA
FDP_FIL_EXT - Test 1	X	X	X	FDP_FIL_EXT.1/UA
FDP_FIL_EXT - Test 2	X	X	X	FDP_FIL_EXT.1/UA
FDP_FIL_EXT - Test 3				Not selected / NA

FDP_PWR_EXT - Test 1	X	X	X	FDP_PWR_EXT.1
FDP_UAI_EXT - Test 1	X	X	X	FDP_UAI_EXT.1
FDP_UAI_EXT - Test 2	X	X	X	FDP_UAI_EXT.1
FDP_UAI_EXT - Test 3				This test is not applicable to this configuration as no KVM uses USB type-C as a console video output.

4 Test Bed Descriptions

4.1 Test Bed # 1

4.1.1 Visual Diagram

Below is a diagram of the components included in the test bed:

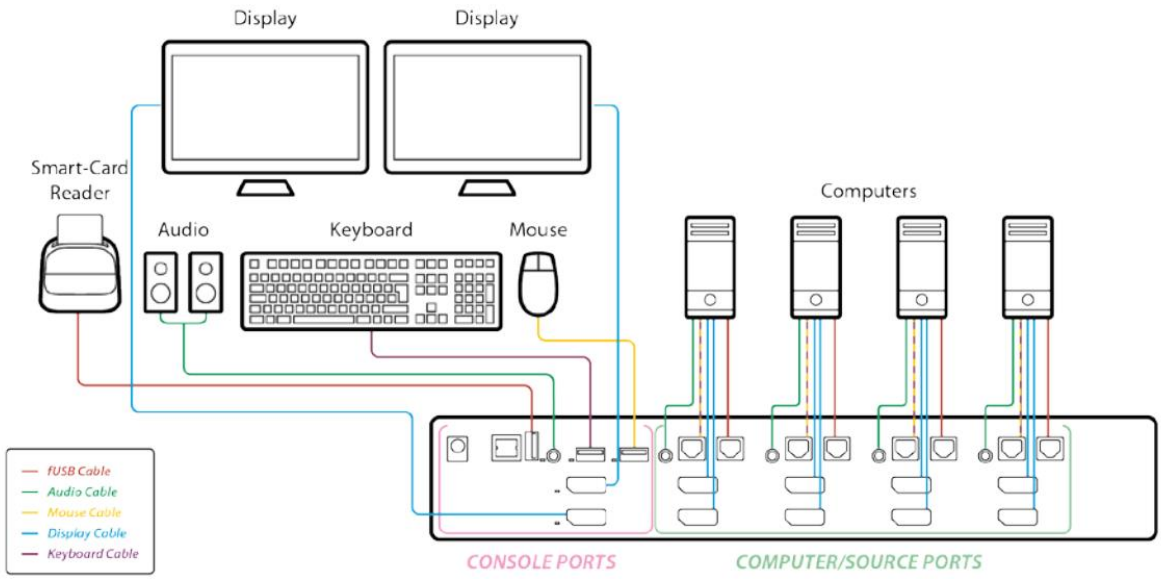

Figure 1 – Test Setup

4.1.2 Test Equipment

The following equipment was used in the testing of the TOE:

Test Equipment
Dell Keyboard with Smart Card Reader KB813T
HP Deskjet 1112 USB Printer
Dr. Meter DC Power Supply HY3005F-3
RIGOL DG1022A Waveform Audio Signal Generator
RIGOL DG1022A Waveform Audio Signal Generator
QuantumData 882E Video Test Generator (DisplayPort)
QuantumData 980 Video Test Generator (HDMI)
TELEDYNE LECROY USB-TMS2-M01-X USB Sniffer
UNIGRAF DPA-400 DisplayPort Aux Channel Monitor
Tektronix TBS1104 Oscilloscope
Fluke 117 True RMS Digital Multimeter
Custom USB Dummy Load
Edifier R980T Multimedia Speaker
PS/2 to USB Adapter
Perixx PeriMice-201 II Optical PS/2 Mouse
MPOW BH323A 3.5mm Headset with USB Connector
Identiv SCR3310 USB UA Device with Power LED

TCL 40” LED Smart TV With Audio Return Channel (ARC)
BYEASY USB 4 Port Hub
Logitech V-U-0018 USB Camera
Steelseries Rival 100 USB Gaming Mouse
Custom BADUSB
Netum USB Barcode Reader
Wireless LAN Dongle
Keweisi USB Detector
3.5mm Microphone
Dell P2319H Monitor (High Resolution Monitor #1)
Asus PA238 Monitor (High Resolution Monitor #2)
Dell Wired Keyboard KB216t
UGREEN VGA to HDMI Adapter
Dell 1907FPc Monitor (Low Resolution Monitor)
Dell Wired Mouse M-UAR DEL 7
Cable Matters VGA to DisplayPort Adapter

Cables

Cable
3.5mm Audio Splitter
Spliced HDMI Cable
Spliced 3.5mm Cable
Spliced USB Type-B Cable
Spliced DisplayPort Cable
Spliced USB Type-C Cable
Spliced USB Type-A Cable

Computers

Name and Hardware	OS	Version	Function
Computer #1 HP ProDesk 600 G4	Windows 10	10.0.19041	Test Workstation – This computer will be connected to the KVM and provide keyboard, mouse, video, audio, and user authentication data when needed.
Computer #2 HP ProDesk 600 G4	Windows 10	10.0.19041	Test Workstation – This computer will be connected to the KVM and provide keyboard, mouse, video, audio, and user authentication data when needed.

Name and Hardware	OS	Version	Function
Lab PC Dell Vostro Desktop	Windows 10	10.0.19041	Lab Workstation – This computer will be external to the TOE and be used in measuring the KVM's data output.

Software

Name	Version
DisplayPort Aux Channel Monitor	2.0
Monitor Asset Manager	2.91.0.1043
SoftMCCS (Monitor Control Console Software)	2.5.0.1087
TrueRTA (Real Time Audio Spectrum Analyzer)	3.5.6
Teledyne Lecroy USB Protocol Suite™	7.60
USBlyzer (USB Analyzer Software)	2.1
Microsoft Device Manager	10.0.19041
Microsoft Notepad	10.0.19041

4.1.3 Test Time & Location

All testing was carried out on-site in Ottawa, Ontario by Acumen Security personnel. Initial receipt and inspection of the TOE occurred in January 2020. The timeline for testing spanned from January 2020 to March 2022. Testing for the TOE was performed during January through March 2020, July 2020, August/September 2021, December 2021, and March through May 2022. For the entire duration of the testing, 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. This was achieved by inspecting the tamper seals, enclosures, and cabling for signs of tampering. All evaluation documentation was always kept with the evaluator. In addition, all the necessary precautions and safety protocols were followed.

4.1.4 Test Environment

The following test environment is in use throughout the testing process. Each device was tested using one Lab workstation, and two test workstations. This will ensure throughout the testing process that at least two ports per TOE can be tested simultaneously. If a TOE has more than 2 ports, then the evaluator shall move the two test workstations over to the next two ports on the TOE and continue testing.

4.1.5 Configuration Information

The following devices were tested:

Product: SCM185DPH

- Name: CYBEX™ SC Universal DP/H Secure Desktop Matrix 2x8 KVM with CAC
- Number of Ports: 8 Ports
- Display Type: DisplayPort, HDMI

Product: SC845DPHC

- Name: CYBEX™ SC Universal DPH + USB-C secure KVM Switch 4-Port Single Display w/CAC
- Number of Ports: 4 Ports
- Display Type: DisplayPort, HDMI

Product: SCMV245DPH

- Name: CYBEX™ SC Universal DP/H Secure 4-Port MultiViewer KVM with CAC
- Number of Ports: 4 Ports
- Display Type: DisplayPort, HDMI

Product: SC945DPH

- Name: CYBEX™ SC Universal DP/H Secure KVM Switch 4-Port Dual Display with CAC
- Number of Ports: 4 Ports
- Display Type: DisplayPort, HDMI

Product: SCAFP0004

- Name: HighSecLabs™ SCAFP0004 Remote Control (CGA26687)
- Number of Buttons: 1 Button
- Computers Supported: Up to 4 computers
- Connection Type: RJ12 Cable

5 Detailed Test Cases (TSS, Isolation Document, and Guidance Activities)

5.1 TSS, Isolation Document, and Guidance Activities (Auditing)

5.1.1 FAU_GEN.1

5.1.1.1 FAU_GEN.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.1.1.2 FAU_GEN.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the audit functionality including which events are audited, what information is saved in each record type, how the records are stored, the conditions in which audit records are overwritten, and the means by which the audit records may be read. Although the TOE may provide an interface for an administrator to view the audit records, this is not a requirement.

Evaluator Findings	The evaluator examined the section 9.1 titled 'Security Audit' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the 'Security Audit' section of the TSS describes in detail the audit functions, including both the RAM logs and the one-time programming (OTP) logs.
	
	From Section 9.1 of the ST: The TOE is equipped with non-volatile memory for the storage of audit records. There are two separate storage areas:
	• Critical RAM and One Time Programming (OTP) Logs
	  • The critical RAM log area stores the following information:
	  ▪ Tampering events – there are six possible event flags Self-test failure – a record of the latest self-test failure is recorded with error code information
	  ▪ Peripheral device rejection
	  ▪ Configuration changes to the CDF whitelist/blacklist made by the administrator
	  ▪ Reset to factory default event
	  ▪ Changes to the primary administrator password
	  • The OTP log maintains the critical events in parallel with the Critical RAM log. This log stores up to 64 events and does not overwrite. It stops recording when the log is full. When this log is full, critical events will only be recorded in the Critical RAM.
	
	• Non-critical (Random Access Memory (RAM)) Logs
	  • Peripheral device acceptance
	  • Non-security related configuration changes
	  • Administrator login
	  • Administrator logout
	  • Creation and removal of administrator accounts
	  • Administrator password changes (other than for the primary administrator)
	  • Password lock events

	• Power up events The audit system starts up with the device which is noted by the power up event. Power down is a hardware mechanism, therefore writing an audit record on power down is not possible. All events include the date and time. Where applicable, the username of the administrator who initiated the action is also recorded. Logs cannot be deleted by the administrator. The critical logs hold up to 64 events. The non-critical logs hold up to 128 events. In both log files, the oldest logs are overwritten when the storage space allocated to the logs becomes full. Audit records can only be read by authorized administrators through the TOE device's terminal mode. The evaluator also noted that power down is a hardware mechanism, and so writing an audit record on power down is not possible. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.1.3 FAU_GEN.1 Guidance 1

Objective	The evaluator shall verify that the operational guidance provides instructions on how the audit logs can be viewed as well as any information needed to interpret the audit logs.
Evaluator Findings	The evaluator examined the Vertiv Technical Bulletin [Tech_Bul] and CC Guidance Supplement [CC_Supp] to determine the verdict of this evaluation activity. The 'Logs and Events' Section 2.2.7 of the Technical Bulletin has a description of the three types of logs [Critical RAM, Non-Critical RAM, and OTP] along with their content and how to interpret them. The 'Terminal Mode' section provides instructions on how to use the interface to access the logs. Logs cannot be deleted by the administrator. The critical logs hold up to 64 events. The non-critical logs hold up to 128 events. In both log files, the oldest logs are overwritten when the storage space allocated to the logs becomes full. Audit records can only be read by authorized administrators through the TOE device's terminal mode. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2 TSS, Isolation Document, and Guidance Activities (User Data Protection)

5.2.1 FDP_AFL_EXT.1

5.2.1.1 FDP_AFL_EXT.1 Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.1.2 FDP_AFL.1 TSS 1

Objective	The evaluator shall check the TSS to verify that the TOE audio function implementation properly filters the audio passing through the TOE.
Evaluator Findings	The evaluator examined the section titled 'Audio Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the section of the TSS indicates that unidirectional flow data diodes prevent audio data flow from an audio device to a selected computer. There is a separate audio interface for each computer. Each interface is electrically isolated from other interfaces, and from other TOE circuitry. These features ensure that the audio filtration specification requirements are met. This SFR includes Table 13 of [MOD_AO_V1.0]. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.1.3 FDP_AFL.1 Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.2 FDP_APC_EXT.1

5.2.2.1 FDP_APC_EXT.1 Isolation Document 1

Objective	The evaluator shall review the Isolation Documentation and Assessment as described in Appendix D of this PP and ensure that it adequately describes the isolation concepts and implementation in the TOE and why it can be relied upon to provide proper isolation between connected computers whether the TOE is powered on or powered off.
Evaluator Findings	The evaluator examined the Vertiv CYBEX™ SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM145DPH, SCM185DPH, SC985DPH, SCMV245DPH, SCMV285DPH Firmware Version 44444-E7E7 Peripheral Sharing Devices Isolation Document. This document adequately describes the proper isolation whether the TOE is powered on or not. The 'Design Description', section 2, and 'Isolation Means Justification', section 3, describe how isolation is achieved. The section 2.3 titled 'Main Components in the Data Path' provides additional information on how isolation is achieved when the device is powered off. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.2.2 FDP_APC_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the conditions under which the TOE enters a failure state.
Evaluator Findings	The evaluator examined the section titled 'Protection of the TSF' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the TSS

	discusses the conditions under which the TOE enters a failure state. The device enters a failure state as a result of a self-test failure or a tampering event. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.2.3 FDP_APC_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes how a user knows when the TOE enters a failure state.
Evaluator Findings	The evaluator examined the [CC_Supp] to determine the verdict of this evaluation activity. This document describes the possible error states as follows, in Section 4.3 'Error State': "As the product powers up, it performs a self-test procedure. Following failure of a self-test, the device will enter an error state. The error state is indicated by sequential flashing of the Light Emitting Diodes and by a clicking noise. At this point, the device will be inoperable. It will not accept input from any peripheral device or pass output to any peripheral device." Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.3 FDP_APC_EXT.1/AO

5.2.3.1 FDP_APC_EXT.1/AO Isolation Document 1

Objective	The evaluator shall examine the Isolation Documentation to determine that it describes the logic under which the TSF permits audio flows from a connected computer to a connected audio output interface.
Evaluator Findings	The evaluator examined the Isolation Document to determine the verdict of this evaluation activity. The Isolation Document includes two figures, (Figure 1 and Figure2) that illustrate the possible data flows. There follows a table, Table 1 Data Flow Description, that provides an explanation of the data flows. Figures 1, 2, 3, 4, 5 characterize the data flows for various TOE configurations (e.g., combiner, switches, etc.) and are part of the isolation justification and indicate the methods used to maintain the data separation. The 'Main Components in the Data Path' section 2.3 provides an explanation of all data flow isolation. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.3.2 FDP_APC_EXT.1/AO Isolation Document 2

Objective	The evaluator shall examine the Isolation Documentation to determine that it describes how the TOE enforces audio output data flow isolation from other TOE functions, such that it is not possible for two computers connected to the TOE to use the TOE to communicate with one another. The description shall ensure the signal attenuation in the extended audio frequency range between any computer audio output interfaces is at least 45 dB measured with a 2V input pure sine wave at the extended audio frequency range, including negative swing signal.
Evaluator Findings	The evaluator examined the Isolation Document to determine the verdict of this evaluation activity. The 'Power Isolation' section 2.4 discusses power isolation. The 'Isolation Means

	Justification' section 3 describes the isolation enforcement policy for various aspects of the TOE. 'Unauthorized Audio to Audio Flow' section 3.5.3 and 'Unauthorized USB to Audio Flow' section 3.54 provide isolation from other TOE functions. Figure 11 shows the physical characteristics. This also ensures that the audio isolation meets the requirement to ensure that the signal attenuation in the extended audio frequency range between computer audio interfaces is at least 45 dB measured with a 2V input pure sine wave at the extended audio frequency range, including negative swing signal. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.3.3 FDP_APC_EXT.1/AO Isolation Document 3

Objective	The evaluator shall examine the Isolation Documentation to determine that it describes how the TOE prevents the audio output signal from traversing the TOE while the TOE is powered off.
Evaluator Findings	The evaluator examined the Isolation Document to determine the verdict of this evaluation activity. The Isolation Document includes two figures, (Figure 1 and Figure2) that illustrate the possible data flows. There follows a table, Table 1 Data Flow Description, that provides an explanation of the data flows. Figures 1, 2, 3, 4, 5 characterize the data flows for various TOE configurations (e.g., combiner, switches, etc.) and are part of the isolation justification and indicate the methods used to maintain the data separation. The 'Main Components in the Data Path' section 2 provides an explanation of all data flow isolation. The 'Unauthorized Audio to Audio Flow' section 3.5.3 describes the design that prevents audio flow when the TOE is powered off. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.3.4 FDP_APC_EXT.1/AO TSS 1

Objective	There are no additional TSS activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.3.5 FDP_APC_EXT.1/AO Guidance 1

Objective	If the ability of the TOE to grant or deny authorization to audio communications is configurable, the evaluator shall verify that the operational guidance describes how to configure the TSF to behave in the manner specified by the SFR. This includes the possibility of both administratively configured TOE settings and any peripherals/connectors that are included with the TOE that cause data flows to behave differently if peripherals are connected through them.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined [2306] sections 1-4, [2307] sections 1-4, [2282] sections 1-4 and [2284] sections 1-5 to determine the verdict of this evaluation activity. Each guidance document

	provides instructions on how to install the TOE properly. The ability to grant or deny authorization to audio communications is not configurable. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.4 FDP_APC_EXT.1/KM

5.2.4.1 FDP_APC_EXT.1/KM Isolation Document 1

Objective	The evaluator shall examine the Isolation Document and verify it describes how the TOE ensures that no data or electrical signals flow between connected computers in both cases (powered on, powered off).
Evaluator Findings	The evaluator examined the Isolation Document to determine the verdict of this evaluation activity. The Isolation Document includes two figures, (Figure 1 and Figure2) that illustrate the possible data flows. There follows a table, Table 1 Data Flow Description, that provides an explanation of the data flows. Figures 1, 2, 3, 4, and 5 characterize the data flows for various TOE configurations (e.g. combiner, switches, etc.) and are part of the isolation justification and indicate the methods used to maintain the data separation. The 'Main Components in the Data Path' section 2.3 provides an explanation of all data flow isolation. The 'Isolation Means Justification' section 3 describes the isolation enforcement policy for various aspects of the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.4.2 FDP_APC_EXT.1/KM TSS 1

Objective	There are no TSS EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.4.3 FDP_APC_EXT.1/KM Guidance 1

Objective	There are no guidance EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.5 FDP_APC_EXT.1/UA

5.2.5.1 FDP_APC_EXT.1/UA Isolation Document 1

Objective	There are no Isolation Document EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable

Verdict	Not Applicable

5.2.5.2 FDP_APC_EXT.1/UA TSS 1

Objective	There are no TSS EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.5.3 FDP_APC_EXT.1/UA Guidance 1

Objective	There are no guidance EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.6 FDP_APC_EXT.1/VI

5.2.6.1 FDP_APC_EXT.1/VI Isolation Document 1

Objective	The evaluator shall examine the Isolation Document and verify it describes how the TOE ensures that no data or electrical signals flow between connected computers in both cases (powered on, powered off).
Evaluator Findings	The evaluator examined the Isolation Document. The Isolation Document includes two figures, (Figure 1 and Figure2) that illustrate the possible data flows. There follows a table, Table 1 Data Flow Description, that provides an explanation of the data flows. Figures 1, 2, 3, 4, and 5 characterize the data flows for various TOE configurations (e.g., combiner, switches, etc.) and are part of the isolation justification and indicate the methods used to maintain the data separation. The 'Main Components in the Data Path' section 2.3 provides an explanation of all data flow isolation. The 'Power Isolation' section 2.4 discusses power isolation. The 'Isolation Means Justification' describes the isolation enforcement policy for various aspects of the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.6.2 FDP_APC_EXT.1/VI TSS 1

Objective	There are no EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.6.3 FDP_APC_EXT.1/VI Guidance 1

Objective	There are no guidance EAs for this component beyond what the PSD PP requires.

Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.7 FDP_CDS_EXT.1(1)

5.2.7.1 FDP_CDS_EXT.1(1) Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.7.2 FDP_CDS_EXT.1(1) TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes how many connected displays may be supported at a time.
Evaluator Findings	The evaluator examined the ST. The 'Physical Scope' section indicates the number of connected displays supported for each TOE device. The 'Video Switching Functionality' section of the TSS indicates which devices support a single display, and which devices support multiple displays. This information is consistent with the claims in FDP_CDS_EXT.1(1). Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.7.3 FDP_CDS_EXT.1(1) Guidance 1

Objective	The evaluator shall examine the operational user guidance and verify that it describes how many displays are supported by the TOE.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [CC_Supp] section 4.6 titled 'Number of Supported Displays' indicates the number of displays supported by each device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.8 FDP_CDS_EXT.1(2)

5.2.8.1 FDP_CDS_EXT.1(2) Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.8.2 FDP_CDS_EXT.1(2) TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes how many connected displays may be supported at a time.
Evaluator Findings	The evaluator examined the ST. The 'Physical Scope' section indicates the number of connected displays supported for each TOE device. The 'Video Switching Functionality' section of the TSS indicates which devices support a single display, and which devices support multiple displays. This information is consistent with the claims in FDP_CDS_EXT.1(2). Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.8.3 FDP_CDS_EXT.1(2) Guidance 1

Objective	The evaluator shall examine the operational user guidance and verify that it describes how many displays are supported by the TOE.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [CC_Supp] section 4.6 titled 'Number of Supported Displays' indicates the number of displays supported by each device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.9 FDP_FIL_EXT.1/KM

5.2.9.1 FDP_FIL_EXT.1/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this SFR.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.9.2 FDP_FIL_EXT.1/KM TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes whether the PSD has configurable or fixed device filtering. [Conditional - If "configurable" is selected in FDP_FIL_EXT.1.1/KM, then:] the evaluator shall examine the TSS and verify that it describes the process of configuring the TOE for whitelisting and blacklisting KM peripheral devices, including information on how this function is restricted to administrators. The evaluator shall verify that the TSS does not allow TOE device filtering configurations that permit unauthorized devices on KM interfaces.
Evaluator Findings	The evaluator examined the section 9.2.2.3 titled 'Keyboard and Mouse Compatible Device Types' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the selection is 'fixed'. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.9.3 FDP_FIL_EXT.1/KM Guidance 1

Objective	[Conditional - If “configurable” is selected in FDP_FIL_EXT.1.1/KM, then:] the evaluator shall examine the guidance documentation and verify that it describes the process of configuring the TOE for whitelisting and blacklisting KM peripheral devices and the administrative privileges required to do this.
Evaluator Findings	The evaluator examined the ST to determine that ‘Configurable’ has not been selected. Therefore, this evaluation activity is not applicable.
Verdict	Not Applicable

5.2.10 FDP_FIL_EXT.1/UA

5.2.10.1 FDP_FIL_EXT.1/UA Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.10.2 FDP_FIL_EXT.1/UA TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes whether the PSD has configurable or fixed device filtering. [Conditional – If “configurable” is selected in FDP_FIL_EXT.1.1/UA, then:] The evaluator shall examine the TSS and verify that it describes the process of configuring the TOE for whitelisting and blacklisting UA peripheral devices, including information on how this function is restricted to administrators.
Evaluator Findings	The evaluator examined the section 9.2.4 titled ‘User Authentication Device Switching Functionality’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the devices have configurable filtering. The ‘User Authentication Device Switching Functionality’ indicates that by default, only standard USB smart-card readers or biometric authentication devices with USB smart-card class interfaces that comply with the USB Organization standard Chip Card Interface Device (CCID) Revision 1.1 or CCID Revision 1.0 will be accepted by the TOE on the fUSB port. It also indicates that the TOE does not include an authentication device but accepts any USB Smart Card device at the fUSB peripheral port. Only USB Type A connections are permitted. The TOE does not support a wireless connection to an authentication device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.10.3 FDP_FIL_EXT.1/UA Guidance 1

Objective	[Conditional – If “configurable” is selected in FDP_FIL_EXT.1.1/UA, then:] the evaluator shall examine the guidance documentation and verify that it describes the process of configuring

	the TOE for whitelisting and blacklisting UA peripheral devices and the administrative privileges required to do this.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The product guides point to the [Tech_Bull] for instructions on whitelisting devices. The 'Configure DPP' section 2.2.3 of the Technical Bulletin describes the steps that an administrator must perform to whitelist or blacklist a device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.11 FDP_IPC_EXT.1

5.2.11.1 FDP_IPC_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.11.2 FDP_IPC_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes how data DisplayPort data is converted.
Evaluator Findings	The evaluator examined the section 9.2.3 titled 'Video Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the video switching functionality. In the discussion it states that for DisplayPort connections, the TOE video function filters the AUX channel by converting it to I2C EDID only. DisplayPort video is converted into an HDMI video stream. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.11.3 FDP_IPC_EXT.1 Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.12 FDP_PDC_EXT.1

5.2.12.1 FDP_PDC_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable

Verdict	Not Applicable

5.2.12.2 FDP_PDC_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the compatible devices for each peripheral port type supported by the TOE. The description must include sufficient detail to justify any PP-Modules that extend this PP and are claimed by the TOE (e.g., if the ST claims the Audio Input PP-Module, then the TSS shall reference one or more audio input devices as supported peripherals).
Evaluator Findings	The evaluator examined the section 9.2 titled 'User Data Protection' in the Security Target to determine the verdict of this evaluation activity. The compatible device type for each peripheral port type is described in the section 9.2.2.3 titled 'Keyboard and Mouse Compatible Device Types', section 9.2.3.1 'Video Compatible Device Types', section 9.2.4.1 'User Authentication Device Compatible Device Types', and section 9.2.5.1 'Audio Compatible Device Types'. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.12.3 FDP_PDC_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS describes the interfaces between the PSD and computers and the PSD and peripherals and ensure that the TOE does not contain wireless connections for these interfaces.
Evaluator Findings	The evaluator confirmed that the ST indicates that there are no wireless peripherals allowed in this configuration. The 'Keyboard and Mouse Compatible Device Types' section 9.2.2.3 indicates that the TOE does not support a wireless connection to a mouse, keyboard or USB hub. The 'Video Compatible Device Types' section 9.2.3.1 indicates that the TOE does not support a wireless connection to a video display. The 'User Authentication Compatible Device Types' section 9.2.4.1 indicates that the TOE does not support a wireless connection to an authentication device. The 'Audio Compatible Device Types' section 9.2.5.1 indicates that the TOE does not support a wireless connection to an audio output device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.12.4 FDP_PDC_EXT.1 TSS 3

Objective	The evaluator shall verify that the list of peripheral devices and interfaces supported by the TOE does not include any prohibited peripheral devices or interface protocols specified in Appendix E.
Evaluator Findings	The evaluator examined the section 9.2 titled 'User Data Protection' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the allowed peripheral devices and protocols in section 9.2.2.3 'Keyboard and Mouse Compatible Device Types', section 9.2.3.1 Video Compatible Device Types', section 9.2.4.1 'User Authentication Compatible Device Types' and section 9.2.5.1 'Audio Compatible Device Types'. The TOE does not allow non-compliant devices.

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

5.2.12.5 FDP_PDC_EXT.1 TSS 4

Objective	The evaluator shall verify that the TSS describes all external physical interfaces implemented by the TOE, and that there are no external interfaces that are not claimed by the TSF.
Evaluator Findings	The evaluator examined the section 9.2 titled 'User Data Protection' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes all physical interfaces to the peripheral devices in section 9.2.2.3 'Keyboard and Mouse Compatible Device Types', section 9.2.3.1 'Video Compatible Device Types', section 9.2.4.1 'User Authentication Compatible Device Types' and section 9.2.5.1 'Audio Compatible Device Types'. The TOE is compliant to the PSD PP Appendix E and does not describe any unclaimed external interfaces. Additionally, the evaluator compared the descriptions in the ST with the image of the devices in the ST, and confirmed that every visible interface was described. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.12.6 FDP_PDC_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance provides clear direction for the connection of computers and peripheral devices to the TOE.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the Quick Install Guides, [2282], [2284], [2306] and [2307] sections 1 and 2 and found that they provide clear instructions describing how to connect peripheral devices to the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.12.7 FDP_PDC_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance provides clear direction for the usage and connection of TOE interfaces, including general information for computer, power, and peripheral devices.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined [2306], [2307], [2282], [2284] and determined that they provide clear instructions on how to connect peripheral devices, power and computers in sections 1 and 2. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.12.8 FDP_PDC_EXT.1 Guidance 3

Objective	The evaluator shall determine if interfaces that receive or transmit data to or from the TOE present a risk that these interfaces could be misused to import or export user data.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The Quick Install Guides provide connectivity details. The [CC_Supp] provides additional instructions on usage, including environmental requirements required to alleviate the risk of data loss in section 1.1. This includes: 'Special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions may not be used with the secure peripheral sharing device.' and 'Microphones must not be plugged into the TOE audio output interfaces.' Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.12.9 FDP_PDC_EXT.1 Guidance 4

Objective	The evaluator shall verify that the operational user guidance describes the visual or auditory indications provided to a user when the TOE rejects the connection of a device.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [2306], [2307] and [2282] in section 4 and [2284] section 5 discuss the acceptance/rejection of a device. When no device is detected, the LED is off. When the TOE rejects a device, an LED on the port blinks green. When the TOE accepts a device, the LED is solid green. There are no audible indications. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.12.10 FDP_PDC_EXT.1 Guidance 1-KM, UA, VI

Objective	The evaluator shall verify that the operational user guidance describes devices authorized for use with the TOE in accordance with the authorized peripheral device connections.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [2306], [2307], [2282], [2284]in sections 1 and 2 indicate the peripheral device type interfaces of the TOE devices. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.13 FDP_PDC_EXT.2/AO

5.2.13.1 FDP_PDC_EXT.2/AO Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.13.2 FDP_PDC_EXT.2/AO TSS 1

Objective	There are no TSS EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.13.3 FDP_PDC_EXT.2/AO Guidance 1

Objective	The evaluator shall verify that the operational guidance describes devices authorized for use with the TOE in accordance with the authorized peripheral device connections.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the [2306], [2307], [2282], [2284] and determined that they indicate the types of peripheral devices supported by the TOE in sections 1 and 2. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.14 FDP_PDC_EXT.2/KM

5.2.14.1 FDP_PDC_EXT.2/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this SFR.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.14.2 FDP_PDC_EXT.2/KM TSS 1

Objective	TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.14.3 FDP_PDC_EXT.2/KM Guidance 1

Objective	Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.15 FDP_PDC_EXT.2/UA

The EAs for this SFR are performed as part of activities for FDP_PDC_EXT.1 above.

5.2.16 FDP_PDC_EXT.2/VI

5.2.16.1 FDP_PDC_EXT.2/VI Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.16.2 FDP_PDC_EXT.2/VI TSS 1

Objective	TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.16.3 FDP_PDC_EXT.2/VI Guidance 1

Objective	Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.17 FDP_PDC_EXT.3/KM

5.2.17.1 FDP_PDC_EXT.3/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this SFR.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.17.2 FDP_PDC_EXT.3/KM TSS 1

Objective	The evaluator shall examine the TSS and verify it describes which types of peripheral devices that the PSD supports.
Evaluator Findings	The evaluator examined the section titled ‘User Data Protection in the Security Target’ to determine the verdict of this evaluation activity. The evaluator confirmed that the TSS describes which peripherals are used in the ‘Keyboard and Mouse Compatible Device Types’, ‘Video Compatible Device Types’, ‘User Authentication Compatible Device Types’ and ‘Audio Compatible Device Types’ sections. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.17.3 FDP_PDC_EXT.3/KM TSS 2

Objective	The evaluator shall examine the TSS to verify that keyboard or mouse device functions are emulated from the TOE to the connected computer.
Evaluator Findings	The evaluator examined the section titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that 'Keyboard and Mouse Switching Functionality' section indicates that the keyboard and mouse function are emulated by the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.17.4 FDP_PDC_EXT.3/KM Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.18 FDP_PDC_EXT.3/VI

5.2.18.1 FDP_PDC_EXT.3/VI Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.18.2 FDP_PDC_EXT.3/VI TSS 1

Objective	TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.18.3 FDP_PDC_EXT.3/VI Guidance 1

Objective	Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.19 FDP_PDC_EXT.4

5.2.19.1 FDP_PDC_EXT.4 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.19.2 FDP_PDC_EXT.4 TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes whether the PSD has internal or external authentication devices.
Evaluator Findings	The evaluator examined the section 9.2.4 titled 'User Authentication Device Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the authentication devices. The TOE accepts external smart card reader devices. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.19.3 FDP_PDC_EXT.4 TSS 2

Objective	Additional evaluation activities for STs that include the selection "external" are performed under FDP_PDC_EXT.1 in PSD PP.
Evaluator Findings	See FDP_PDC_EXT.1
Verdict	Not Applicable

5.2.19.4 FDP_PDC_EXT.4 Guidance 1

Objective	There are no guidance evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.20 FDP_PUD_EXT.1

5.2.20.1 FDP_PUD_EXT.1 Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.20.2 FDP_PUD_EXT.1 TSS 1

Objective	The evaluator shall verify the TSS states that the TOE does not supply power to an unauthorized device connected to the analog audio output interface.
Evaluator Findings	The evaluator examined the section 9.2.5 titled 'Audio Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that the TOE does not supply power to the analog audio output interface, and cannot be configured to do so. Therefore, it cannot be used to supply power to an unauthorized device on that interface. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.20.3 FDP_PUD_EXT.1 TSS 2

Objective	The evaluator shall also verify that the TOE cannot be configured to supply power to a device connected to the analog audio output interface.
Evaluator Findings	The evaluator examined the section 9.2.5 titled 'Audio Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that the TOE does not supply power to the analog audio output interface, and cannot be configured to do so. Therefore, it cannot be used to supply power to an unauthorized device on that interface. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.20.4 FDP_PUD_EXT.1 Guidance 1

Objective	The evaluator shall verify that the guidance states that a microphone should never be connected to the TOE's analog audio output interface.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [CC_Supp] indicates that microphones must not be plugged into the TOE audio output interfaces in the 'Operational Environment' section 1.1. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.21 FDP_PWR_EXT.1

5.2.21.1 FDP_PWR_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.21.2 FDP_PWR_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS and verify that the connected computer does not power the TOE.
Evaluator Findings	The evaluator examined the section 9.2.4 titled 'User Authentication Device Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that the user authentication device must be able to receive power from the TOE. An external power source, such as power from the connected computer, is prohibited for this interface. This section also indicates that the TOE does not receive power from the computer user authentication device interface. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.21.3 FDP_PWR_EXT.1 Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.22 FDP_RDR_EXT.1

5.2.22.1 FDP_RDR_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.22.2 FDP_RDR_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes how the TSF identifies and rejects a device that attempts to enumerate again as a different device.
Evaluator Findings	The evaluator examined the section 9.2.2 titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses Keyboard and Mouse Enumeration and indicates that a USB keyboard is connected to the TOE keyboard host emulator through the console keyboard port. The keyboard host emulator is a microcontroller which enumerates the connected keyboard and verifies that it is a permitted device type. This section also states that the USB mouse is connected to the TOE mouse host emulator through the USB mouse port. The mouse host emulator is a microcontroller which enumerates the connected mouse and verifies that it is a permitted device type. Section 9.2.2.4 states "If a connected device attempts to re-enumerate as a different USB device type, it will be rejected by the TOE." Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.22.3 FDP_RDR_EXT.1 Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.23 FDP_RIP_EXT.1

5.2.23.1 FDP_RIP_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.23.2 FDP_RIP_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS includes a Letter of Volatility that provides the following information: • Which TOE components have non-volatile memory, the non-volatile memory technology, manufacturer/part number, and memory sizes; • Any data and data types that the TOE may store on each one of these components; • Whether or not each one of these parts is used to store user data and how this data may remain in the TOE after power down; and • Whether the specific component may be independently powered by something other than the TOE (e.g., by a connected computer). Note that user configuration and TOE settings are not considered user data for purposes of this requirement.
Evaluator Findings	The evaluator examined the titled 'Letter of Volatility' in the Security Target to determine the verdict of this evaluation activity. The Letter of Volatility is provided as Annex A in the Security Target. The evaluator confirmed that this section lists each component, its function, manufacture and part number, the type of data stored and whether the storage is volatile, or non-volatile. It also indicates the power source. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.23.3 FDP_RIP_EXT.1 TSS 2

Objective	The evaluator shall verify that the Letter of Volatility provides assurance that user data is not stored in TOE non-volatile memory or storage.

Evaluator Findings	The evaluator examined the section titled 'Letter of Volatility' in the Security Target to determine the verdict of this evaluation activity. The Letter of Volatility is provided as Annex A in the Security Target. The evaluator confirmed that this section indicates that user data is not stored in non-volatile memory or storage. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.23.4 FDP_RIP_EXT.1 Guidance 1

Objective	There are no guidance Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.24 FDP_RIP.1/KM

5.2.24.1 FDP_RIP.1/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.24.2 FDP_RIP.1/KM TSS 1

Objective	The evaluator shall verify that the TSS indicates whether or not the TOE has user data buffers.
Evaluator Findings	The evaluator examined the section titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that the Serial Random Access Memory (SRAM) in the host and device emulator circuitry stores USB Host stack parameters and up to the last 4 key codes. User data may be briefly retained; however, there are no data buffers. Data is erased during power off of the KVM, and when the user switches channels. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.24.3 FDP_RIP.1/KM TSS 2

Objective	The evaluator shall verify that the TSS describes how all keyboard data stored in volatile memory is deleted upon switching computers.
Evaluator Findings	The evaluator examined the section 9.2.2.2 titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that data is erased during power off of the KVM, and when the user switches channels. When the TOE switches from one computer to another, the system controller ensures that the keyboard and mouse stacks are deleted, and that any data received from the keyboard in the first 100 milliseconds following switching is

	deleted. This is done to ensure that any data buffered in the keyboard microcontroller is not passed to the newly selected computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.24.4 FDP_RIP.1/KM Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.25 FDP_RIP_EXT.2

5.2.25.1 FDP_RIP_EXT.2 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.25.2 FDP_RIP_EXT.2 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE's reaction to memory purge or restore factory defaults.
Evaluator Findings	The evaluator examined the section 9.2.1.3 titled 'Residual Information Protection' in the Security Target to determine the verdict of this evaluation activity. When the Reset to Factory Default command is issued, the following actions take place: • All peripheral devices are logically disconnected from the selected computer • The front panel LEDs blink together • The TOE resets, purging the appropriate data • The TOE performs a normal power up and self-test sequence When the device completes the reboot, the peripherals are connected to channel #1 and all default settings are restored. The data in the critical logs, and the primary administrator username and password data are maintained in the OTP Memory of the System Controller. All other data is purged. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.25.3 FDP_RIP_EXT.2 TSS 2

Objective	The evaluator shall verify that the Letter of Volatility included in the TSS describes the effect that the TOE Restore Factory Default function has on each component listed in the Letter of Volatility.
Evaluator Findings	The evaluator examined the section titled 'Letter of Volatility' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the 'Letter of Volatility' indicates the effect of the restore to factory default function on each component. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.25.4 FDP_RIP_EXT.2 Guidance 1

Objective	The evaluator shall check that the operational user guidance provides a method to purge TOE memory or to restore factory default settings.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Terminal Mode Options'section 2.2 and 'Reset to Factory Defaults' section 2.2.6 of the [Tech_Bull] describes the factory reset function and what that entails. The 'Selected Channel at Startup' section 4.4 of the [CC_Supp] states that Channel 1 is selected by default after a factory reset. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.26 FDP_SPR_EXT.1/DP

5.2.26.1 FDP_SPR_EXT.1/DP Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.26.2 FDP_SPR_EXT.1/DP TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.
Evaluator Findings	The evaluator examined the section 9.2.3 titled 'Video Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses the allowed and blocked sub-protocols supported for the DisplayPort protocol. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.26.3 FDP_SPR_EXT.1/DP Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable

5.2.27 FDP_SPR_EXT.1/HDMI

5.2.27.1 FDP_SPR_EXT.1/HDMI Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.27.2 FDP_SPR_EXT.1/HDMI TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.
Evaluator Findings	The evaluator examined the section 9.2.3 titled 'Video Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses the allowed and blocked sub-protocols supported for the HDMI protocol. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.27.3 FDP_SPR_EXT.1/HDMI Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.28 FDP_SPR_EXT.1/USB

5.2.28.1 FDP_SPR_EXT.1/USB Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.28.2 FDP_SPR_EXT.1/USB TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.

Evaluator Findings	The evaluator examined the section 9.2.3 titled 'Video Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses the allowed and blocked sub-protocols supported for the USB Type-C with DisplayPort as an alternate function protocol. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.28.3 FDP_SPR_EXT.1/USB Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.29 FDP_SWI_EXT.1

5.2.29.1 FDP_SWI_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.29.2 FDP_SWI_EXT.1 TSS 1

Objective	If the ST includes the selection the "TOE supports only one connected computer", the evaluator shall verify that the TSS indicates that the TOE supports only one connected computer.
Evaluator Findings	The evaluator examined FDP_SWI_EXT.1 in the 'Security Functional Requirements' section 6.2.2.24 of the Security Target. The selection 'switching can be initiated only through express user action' has been made. Since 'TOE supports only one connected computer' is not selected, this evaluation activity is considered not applicable.
Verdict	Not Applicable

5.2.29.3 FDP_SWI_EXT.1 TSS 2

Objective	If the ST includes the selection "switching can be initiated only through express user action", the evaluator shall verify that the TSS describes the TOE supported switching mechanisms and that those mechanisms can be initiated only through express user action.
Evaluator Findings	The evaluator examined the section 1.4 titled 'TOE Overview' and the TSS section 9.2.1 titled 'System Controller' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the 'TOE Overview' states that the Vertiv Secure Peripheral Sharing Devices (PSD) allow users to share keyboard, video, and mouse peripherals between a number of connected computers. The TSS has been written for multiple connected computers and explains how the user is able to conduct the switching. The 'System Controller' section

	describes the switching mechanism. All devices may be switched using the front panel buttons, a remote control and the SCMV245DPH and SCMV285DPH devices may be switched with a peripheral device using a guard. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.29.4 FDP_SWI_EXT.1 Guidance 1

Objective	If the ST includes the selection "switching can be initiated only through express user action", the evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The switching mechanisms are described in the [2306], [2307], and [2282] section 5 and in [2284] section 6. Each of these guides includes instructions on how the user performs switching. The [CC_Supp] mentions that a remote is used with the TOE in the 'Remote Control' section. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.30 FDP_SWI_EXT.2(1)

5.2.30.1 FDP_SWI_EXT.2(1) Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.30.2 FDP_SWI_EXT.2(1) TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE supported switching mechanisms. The evaluator shall verify that the TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. The evaluator shall verify that the described switching mechanisms can be initiated only through express user action according to the selections.
Evaluator Findings	The evaluator examined the section 9.2.1 titled 'System Controller' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that all devices may be switched using the front panel buttons and the remote control. Switching can only be initiated through express user action. The TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.30.3 FDP_SWI_EXT.2(1) Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms. The evaluator shall verify that the operational user guidance does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The switching mechanisms are described in [2282] section 5 and in [2284] section 6. Each of these guides includes instructions on how the user performs switching. The [CC_Supp] mentions that a remote is used with the TOE in the 'Remote Control' section. The evaluator reviewed all applicable guidance and confirmed that it does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. [CC_Supp] clarifies that the cursor navigation switching feature is not supported on the SCM185DPH. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.31 FDP_SWI_EXT.2(2)

5.2.31.1 FDP_SWI_EXT.2(2) Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.31.2 FDP_SWI_EXT.2(2) TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE supported switching mechanisms. The evaluator shall verify that the TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. The evaluator shall verify that the described switching mechanisms can be initiated only through express user action according to the selections.
Evaluator Findings	The evaluator examined the section 9.2.1 titled 'System Controller' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the SCMV245DPH and SCMV285DPH devices may be switched using console buttons, remote control or a peripheral device using a guard. Use of the guard is described in the section titled 'System Controller'. Switching can only be initiated through express user action. The TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.31.3 FDP_SWI_EXT.2(2) Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms. The evaluator shall verify that the operational user guidance does not

	include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The switching mechanisms are described in the [2306] section 5, and [2307] section 5. Each of these guides includes instructions on how the user performs switching. The [CC_Supp] mentions that a remote is used with the TOE in the 'Remote Control' section. The evaluator reviewed all applicable guidance and confirmed that it does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.32 FDP_SWI_EXT.3

5.2.32.1 FDP_SWI_EXT.3 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.32.2 FDP_SWI_EXT.3 TSS 1

Objective	The evaluator shall verify that the TSS does not indicate that keyboard and mouse devices may be switched independently to different connected computers.
Evaluator Findings	The evaluator examined the section 9.2.2.2 titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses keyboard and mouse switching. The 'TOE Access' section 9.5 indicates that the TOE user switches between computers by pressing the corresponding front panel button on the device. The TSS does not indicate that keyboard and mouse devices may be switched independently to different connected computers. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.32.3 FDP_SWI_EXT.3 Guidance 1

Objective	The evaluator shall verify that the guidance does not describe how to switch the keyboard and mouse devices independently to different connected computers.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'User Roles' section 4.1 of the [CC_Supp] states that the user has access to the switching capability. All switching is performed manually. There are no mentions made anywhere in the guidance documentation that keyboard and mouse devices may be switched independently to different computers. Based on these findings, this evaluation activity is considered satisfied.

Verdict	Pass

5.2.33 FDP_TER_EXT.1

5.2.33.1 FDP_TER_EXT.1 Isolation Document 1

Objective	There are no Isolation Document activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.33.2 FDP_TER_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS and verify that the TOE terminates an open session upon removal of the authentication element.
Evaluator Findings	The evaluator examined the section 9.2.4 titled 'User Authentication Device Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that removal of the authentication device will also close the authentication session. Once the authentication device is removed, the session is terminated. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.33.3 FDP_TER_EXT.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon removal of the authentication element.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Authentication Device Switching and Removal' section 4.7 of the [CC_Supp] indicates that an open authentication device session is terminated on removal of the authentication device, or when the device is switched to a different computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.34 FDP_TER_EXT.2

5.2.34.1 FDP_TER_EXT.2 Isolation Document 1

Objective	There are no Isolation Document activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.34.2 FDP_TER_EXT.2 TSS 1

Objective	The evaluator shall examine the TSS and verify that the TOE terminates an open session upon removal of the authentication device.
Evaluator Findings	The evaluator examined the section 9.2.4 titled 'User Authentication Device Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that, following triggering of the anti-tampering function, following a failed self-test, or when the TOE is powered off, all user authentication device data paths are isolated through the peripheral multiplexer. These events effectively disconnect any open authentication session. Removal of the authentication device will also close the authentication session. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.34.3 FDP_TER_EXT.2 Guidance 1

Objective	The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon removal of the authentication device.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Authentication Device Switching and Removal' section 4.7 of the [CC_Supp] indicates that an open authentication device session is terminated on removal of the authentication device, or when the device is switched to a different computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.35 FDP_TER_EXT.3

5.2.35.1 FDP_TER_EXT.3 Isolation Document 1

Objective	The evaluator shall examine the isolation document and verify that it describes how power is reset to the user authentication device upon switching.
Evaluator Findings	The evaluator examined the Isolation Document section 3.9 titled 'Unauthorized Flow Designator S and T' to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that when a user switches from one connected computer to another, the TOE resets the user authentication device through power supply switching, i.e. a temporary power dip. This is performed by High-side Power switches on the System Controller board that switch 5V power to the fUSB device jack. A load field-effect transistor (FET) shorts the supply voltage to the ground to quickly discharge any capacitance in the TOE or in the connected device to a level below 0.5V. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.35.2 FDP_TER_EXT.3 TSS 1

Objective	The evaluator shall examine the TSS and verify that the TOE terminates an open session upon switching to a different computer.

Evaluator Findings	The evaluator examined the section 9.2.4 titled 'User Authentication Device Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that when a user switches from one connected computer to another, the TOE resets the user authentication device through power supply switching (effectively closing the authentication session), i.e. a temporary power dip. This is performed by High-side Power switches on the System Controller board that switch 5V power to the fUSB device jack. A load field-effect transistor (FET) shorts the supply voltage to the ground to quickly discharge any capacitance in the TOE or in the connected device to a level below 0.5V. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.35.3 FDP_TER_EXT.3 Guidance 1

Objective	The evaluator shall examine the guidance documentation and verify that the TOE terminates an open session upon switching to a different computer.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Authentication Device Switching and Removal' section 4.7 of the [CC_Supp] indicates that an open authentication device session is terminated when the device is switched to a different computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.36 FDP_UAI_EXT.1

5.2.36.1 FDP_UAI_EXT.1 Isolation Document 1

Objective	The evaluator shall examine the Isolation Documentation and verify that it describes how the TOE enforces user authentication isolation from other TOE USB functions.
Evaluator Findings	The evaluator examined the Isolation Document section 3.8 titled 'Unauthorized Flow Designator R' to determine the verdict of this evaluation activity. The evaluator confirmed that Figure 13 and the accompanying text describe authentication device isolation. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.36.2 FDP_UAI_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS and verify that it states that the TOE has separate USB connections for user authentication functions and any other USB functions.
Evaluator Findings	The evaluator examined the section 9.2.4 titled 'User Authentication Device Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that authentication device functions use independent circuitry and power planes. They are separate and physically isolated from the keyboard, mouse, or display and audio switching functions. Based on these findings, this evaluation activity is considered satisfied.

Verdict	Pass

5.2.36.3 FDP_UAI_EXT.1 Guidance 1

Objective	The evaluator shall examine the guidance and verify that it states that the TOE has separate USB connections for user authentication functions and any other USB functions.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [2306], [2307], [2282] and [2284] provide diagrams showing a separate USB Type A Dedicated Peripheral Port for user authentication devices. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.37 FDP_UDF_EXT.1/AO

5.2.37.1 FDP_UDF_EXT.1/AO Isolation Document 1

Objective	The evaluator shall examine the Isolation Documentation to determine that it describes how the TOE enforces audio output data flow isolation from other TOE functions, such that the audio output peripheral interface is unidirectional and no data can be routed from a connected peripheral back to a connected computer. The description shall ensure the signal attenuation between any TOE audio output peripheral device interface and any other TOE computer audio output interface is at least 45 dB measured with a 2V input pure sine wave at the extended audio frequency range, including negative swing signal.
Evaluator Findings	The evaluator examined the Isolation Document section 3.5.3 titled 'Unauthorized Audio to Audio Flow' and the section 3.5.4 titled 'Unauthorized USB to Audio Flow' to determine the verdict of this evaluation activity. The evaluator confirmed that the 'Unauthorized Audio to Audio Flow' section indicates that isolated interfaces and components are used, as are audio data diodes. There are no shared parts. It then explains how isolation is achieved. The 'Unauthorized USB to Audio Flow' section describes how the audio output is isolated from the USB paths. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.37.2 FDP_UDF_EXT.1/AO TSS 1

Objective	There are no TSS EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.37.3 FDP_UDF_EXT.1/AO Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable

Verdict	Not Applicable

5.2.38 FDP_UDF_EXT.1/KM

5.2.38.1 FDP_UDF_EXT.1/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.38.2 FDP_UDF_EXT.1/KM TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes if and how keyboard Caps Lock, Num Lock, and Scroll Lock indications are displayed by the TOE and to verify that keyboard internal LEDs are not changed by a connected computer.
Evaluator Findings	The evaluator examined the section 9.2.2 titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section explains how the flows to the keyboard/mouse are unidirectional. It states that the TOE uses optical data diodes to enforce a unidirectional data flow from the user peripherals to the coupled hosts and uses isolated device emulators to prevent data leakage through the peripheral switching circuitry. It also indicates that the use of Caps lock, Num lock and Scroll lock are indicated on the TOE front panel. Keyboard internal LEDs are not changed by a connected computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.38.3 FDP_UDF_EXT.1/KM TSS 2

Objective	The evaluator shall examine the TSS to verify that keyboard and mouse functions are unidirectional from the TOE keyboard/mouse peripheral interface to the TOE keyboard/mouse computer interface.
Evaluator Findings	The evaluator examined the section 9.2.2 titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section explains how the flows to the keyboard/mouse are unidirectional. It states that the TOE uses optical data diodes to enforce a unidirectional data flow from the user peripherals to the coupled hosts and uses isolated device emulators to prevent data leakage through the peripheral switching circuitry. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.2.38.4 FDP_UDF_EXT.1/KM Guidance 1

Objective	There are no guidance EAs for this component.

Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.39 FDP_UDF_EXT.1/VI

5.2.39.1 FDP_UDF_EXT.1/VI Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.39.2 FDP_UDF_EXT.1/VI TSS 1

Objective	There are no TSS EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.2.39.3 FDP_UDF_EXT.1/VI Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.3 TSS, Isolation Document, and Guidance Activities (Identification and Authentication)

5.3.1 FIA_UAU.2

This SFR is evaluated by the Evaluation Activities in FMT_MOF.1 below.

5.3.2 FIA_UID.2

This SFR is evaluated by the Evaluation Activities in FMT_MOF.1 below.

5.4 TSS, Isolation Document, and Guidance Activities (Security Management)

5.4.1 FMT_MOF.1

5.4.1.1 FMT_MOF.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.4.1.2 FMT_MOF.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the mechanism for preventing non-administrators from accessing the administrative functions stated above.
Evaluator Findings	The evaluator examined the section 9.3 titled 'Identification and Authentication and Security Management' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that there is a single administrator role. In order to access administrative functions, the user must have an administrator username and password. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.1.3 FMT_MOF.1 TSS 2

Objective	If the TSF provides multiple administrative roles, the evaluator shall verify that the authorized behavior for each separate administrative role is described.
Evaluator Findings	The evaluator examined the section 9.3 titled 'Identification and Authentication and Security Management' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that there is a single administrator role. An account with this role may be used to perform the following administrative tasks: • Modify the CDF for authentication devices • Manage administrator accounts (change password, create administrator account) • Reset to factory defaults – note that this does not reset the username and password of the primary administrator, and does not reset the critical logs Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.1.4 FMT_MOF.1 TSS 3

Objective	The evaluator shall check the TSS to verify that it describes at least the following: a) Administrator name limitations and syntax requirements; b) Administrator password limitations and syntax requirements; c) Restoring lost name or password; d) Initial setting of administrator credentials; e) Logon success, fail limitations, and logging; and f) All functions identified in the above assignment.
Evaluator Findings	The evaluator examined the section 9.3 titled 'Identification and Authentication and Security Management' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the administrator account username and password limitations. For these accounts, usernames must be between 8 and 11 characters in length, and may be made up of uppercase and lowercase letters and numbers.

	The primary administrator has a default password which is changed on first use. This account does not revert to default but maintains the administrator's account when an RFD is performed. The administrator's password must be between 8 and 15 characters in length and may contain uppercase letters, lowercase letters, numbers or any of the following special characters: '!', '@', '#', '$', '%', '^', '&', '*', '(', ')', '-', or '_'. The password must contain at least one uppercase letter, one lowercase letter, one number and one special character. Lost passwords are irrecoverable. The user is locked out after three failed login attempts. The user may cycle the device power and try again. All password related events are logged. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.1.5 FMT_MOF.1 Guidance 1

Objective	The evaluator shall check the user and administrative guidance to verify that the administrative functions described above are only available to identified administrators. If the TSF provides multiple administrative roles, the evaluator shall verify that the authorized behavior for each separate administrative role is described.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Accessing Terminal Mode' section 2.1 of the [Tech_Bull] contains the information regarding passwords. This manual is intended only for use by the administrator. A user must be in possession of an administrative username and password in order to access the functionality described in this guide. Only one administrative role is supported. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.2 FMT_SMF.1

5.4.2.1 FMT_SMF.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.4.2.2 FMT_SMF.1 TSS 1

Objective	The evaluator shall check to ensure the TSS describes the management functions available to the administrators and user TOE configurations and how they are used by the TOE.
Evaluator Findings	The evaluator examined the section 9.3 titled 'Identification and Authentication and Security Management' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that there is a single administrator role. An account with this role may be used to perform the following administrative tasks:

	• Modify the CDF for authentication devices • Manage administrator accounts (change password, create administrator account) • Reset to factory defaults – note that this does not reset the username and password of the primary administrator, and does not reset the critical logs Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.2.3 FMT_SMF.1 Guidance 1

Objective	The evaluator shall check that every management function mandated in the ST for this requirement is described in the operational user guidance and that the description contains the information required to perform the management duties associated with each management function.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Terminal Mode' section 2 of the [Tech_Bull] contains instructions on how to perform administrative functions. The administrative interface is called 'Terminal Mode'. This guide provides instructions on how to perform administrative functions using Terminal Mode. This includes modification of the CDF for authentication devices ('Configure DPP' section 2.2.3), management of administrator accounts ('Account Management' section2.2.5) and Reset to factory default ('Reset to Factory Defaults' section 2.2.6). Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.3 FMT_SMR.1

Refer to the Evaluation Activities of FMT_MOF.1.1 above.

5.5 TSS, Isolation Document, and Guidance Activities (Protection of the TSF)

5.5.1 FPT_FLS_EXT.1(1)

Not Applicable. This SFR is evaluated in conjunction with FPT_TST.1.

5.5.2 FPT_FLS_EXT.1(2)

Not Applicable. This SFR is evaluated in conjunction with FPT_TST.1.

5.5.3 FPT_NTA_EXT.1

5.5.3.1 FPT_NTA_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.5.3.2 FPT_NTA_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that the TSS documents that connected computers and peripherals do not have access to TOE software, firmware, and TOE memory, except as described above.
Evaluator Findings	The evaluator examined the section 9.4.1 titled 'No Access to TOE' in the Security Target to determine the verdict of this evaluation activity. The TSS states: "Connected computers do not have access to TOE firmware or memory, with the following exceptions: • EDID data is accessible to connected computers from the TOE • Authorized administrators use a connected computer to access configuration data and settings • Authorized administrators use a connected computer to access TOE audit records" The evaluator confirmed that this section also indicates that firmware is executed on SRAM with the appropriate protections to prevent external access and tampering of code or stacks. Firmware cannot be read or rewritten using JTAG tools. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.3.3 FPT_NTA_EXT.1 Guidance 1

Objective	The evaluator shall check the operational user guidance to ensure any configurations required to comply with this SFR are defined.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'User Roles' section 4.1 of the CC Guidance Supplement provides a description of the features available to users. No additional configuration is required to comply with this SFR as stated in this section. The [2306], [2282] and [2284] include a warning that there is active tamper detection in the device and that tamper evident seals are used on the device. The [2307] instructs users of the SCMV245DPH and SCMV285DPH devices to ensure that the tamper-evident labels are intact before use. All warnings and instructions are on page 1 prior to any sections. The tamper seals and anti-tamper mechanism ensure that no access is provided to the internal components or firmware without leaving observable tamper evidence or completely disabling the unit. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.4 FPT_PHP.1

5.5.4.1 FPT_PHP.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.

Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.5.4.2 FPT_PHP.1 TSS 1

Objective	The evaluator shall verify that the TSS indicates that the TOE provides unambiguous detection of physical tampering of the TOE enclosure and TOE remote controller (if applicable). The evaluator shall verify that the TSS provides information that describes how the TOE indicates that it has been tampered with.
Evaluator Findings	The evaluator examined the section 9.4.2.1 titled 'Passive Detection of Physical Tampering' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the tamper evident seals are described in this section. If a seal is removed, the word VOID appears to indicate the TOE has been tampered with. The remote control also has a holographic Tampering Evident Label placed at a critical location. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.4.3 FPT_PHP.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes the mechanism by which the TOE provides unambiguous detection of physical tampering and provides the user with instructions for verifying that the TOE has not been tampered with.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [2306], [2282] and [2284] include a warning that there is active tamper detection in the device and that tamper evident seals are used on the device. The [2307] instructs users to ensure that the tamper-evident labels are intact before use. Users are directed to contact Technical Support if the enclosure appears to have been tampered with. All warnings and instructions are on page 1 prior to any sections. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.5 FPT_PHP.3

5.5.5.1 FPT_PHP.3 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.5.5.2 FPT_PHP.3 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE's reaction to opening the device enclosure or damaging/exhausting the anti-tampering battery associated with the enclosure.

Evaluator Findings	The evaluator examined the section 9.4.2.2 titled 'Resistance to Physical Attack' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses the TOE's response to a tamper event. If the enclosure is opened, the anti-tamper circuitry causes a fuse on the system controller to melt and renders the TOE inoperable. Additionally, if the self-test detects that the battery is depleted or failing, the anti-tampering function will be triggered. This functionality applies to the SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM145DPH, SCM185DPH, SC985DPH and the remote control devices. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.5.3 FPT_PHP.3 Guidance 1

Objective	The evaluator shall examine the operational user guidance and verify that the guidance provides users with information on how to recognize a device where the anti-tampering functionality has been activated.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. [2306], [2282] and [2284] include a warning that there is active tamper detection in the device. Users are instructed to contact Technical Support when the tamper event occurs. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.5.4 FPT_PHP.3 Guidance 2

Objective	The evaluator shall verify that the operational user guidance warns the user of the actions that will cause the anti-tampering functionality to disable the device.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The [2306], [2282] and [2284] include a warning that there is active tamper detection in the device. Users are instructed that if the enclosure appears to have been tampered with, or if all the port LEDs flash sequentially, they are to contact Technical Support. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.6 FPT_STM.1

5.5.6.1 FPT_STM.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.5.6.2 FPT_STM.1 TSS 1

Objective	The evaluator shall check to ensure the TSS describes how the TOE provides reliable timestamps.
Evaluator Findings	The evaluator examined the section 9.4.3 titled 'Reliable Timestamps' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that the devices have a real-time clock powered by a battery and the time is set during production. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.6.3 FPT_STM.1 Guidance 1

Objective	The evaluator shall check that the operational user guidance describes how the TOE provides reliable timestamps and if there are any management functions for configuring the time.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Timestamps' section 4.5 of the [CC_Supp] states that each device includes a real-time clock powered by a battery. The time is set during production. There are no management functions that allow configuration of time. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.7 FPT_TST.1(1)

5.5.7.1 FPT_TST.1(1) Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.5.7.2 FPT_TST.1(1) TSS 1

Objective	The evaluator shall verify that the TSS describes the self- tests that are performed on start up or on reset (if "upon reset button activation" is selected). The evaluator shall verify that the self-tests cover at least the following: a) a test of the user interface – in particular, tests of the user control mechanism (e.g., checking that the front panel push-buttons are not jammed); and b) if "active anti-tamper functionality" is selected, a test of any antitampering mechanism (e.g., checking that the backup battery is functional).
Evaluator Findings	The evaluator examined the section 9.4.4 titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses the self-test and what it encompasses: • Verification of the front panel push-buttons

	• Verification of the active anti-tampering functionality, including the continued functionality of the backup battery (where applicable) • Verification of the integrity of the microcontroller firmware • Verification of computer port isolation. This is tested by sending test packets to various interfaces and attempting to detect this traffic at all other interfaces Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.7.3 FPT_TST.1(1) TSS 2

Objective	The evaluator shall verify that the TSS describes how the TOE ensures a shutdown upon a self-test failure or a failed anti-tampering function, if present. If there are instances when a shutdown does not occur (e.g., a failure is deemed non-security relevant), those cases are identified and a rationale is provided explaining why the TOE's ability to enforce its security policies is not affected.
Evaluator Findings	The evaluator examined the section 9.4.4 titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that if the self-test fails, the front panel LEDs blink and the TOE makes a clicking sound. The TOE disables the PSD switching functionality, and enters a disabled state. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.7.4 FPT_TST.1(1) TSS 3

Objective	The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.
Evaluator Findings	The evaluator examined the section 9.4.4 titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that if the self test fails, the front panel LEDs blink and the TOE makes a clicking sound. The TOE disables the PSD switching functionality, and enters a disabled state. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.7.5 FPT_TST.1(1) TSS 4

Objective	The evaluator shall examine the TSS to verify that it describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.
Evaluator Findings	The evaluator examined the section 9.4.4 titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that the TOE can be rebooted to rerun the self test to clear the error. All errors are logged.

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

5.5.7.6 FPT_TST.1(1) Guidance 1

Objective	The evaluators shall verify that the operational user guidance describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' section 4.2 of the [CC_Supp] provides instructions on how to initiate a self test, and how to exit self test mode. In the case of a failure, users are directed to contact Vertiv Technical Support. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.8 FPT_TST.1(2)

5.5.8.1 FPT_TST.1(2) Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.5.8.2 FPT_TST.1(2) TSS 1

Objective	The evaluator shall verify that the TSS describes the self- tests that are performed on start up or on reset (if "upon reset button activation" is selected). The evaluator shall verify that the self-tests cover at least the following: a) a test of the user interface – in particular, tests of the user control mechanism (e.g., checking that the front panel push-buttons are not jammed); and b) if "active anti-tamper functionality" is selected, a test of any antitampering mechanism (e.g., checking that the backup battery is functional).
Evaluator Findings	The evaluator examined the section 9.4.4 titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses the self-test and what it encompasses: • Verification of the front panel push-buttons • Verification of the integrity of the microcontroller firmware • Verification of computer port isolation. This is tested by sending test packets to various interfaces and attempting to detect this traffic at all other interfaces If the self-test fails the front panel LEDs blink and the TOE makes a clicking sound. The TOE can be rebooted to clear the error and the self-test is rerun. All errors are logged. Active anti-tampering functionality is not selected for this iteration of the SFR.

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

5.5.8.3 FPT_TST.1(2) TSS 2

Objective	The evaluator shall verify that the TSS describes how the TOE ensures a shutdown upon a self-test failure or a failed anti-tampering function, if present. If there are instances when a shutdown does not occur (e.g., a failure is deemed non-security relevant), those cases are identified and a rationale is provided explaining why the TOE's ability to enforce its security policies is not affected.
Evaluator Findings	The evaluator examined the section 9.4.4 titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that if the self test fails, the front panel LEDs blink and the TOE makes a clicking sound. The TOE disables the PSD switching functionality, and enters a disabled state. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.8.4 FPT_TST.1(2) TSS 3

Objective	The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.
Evaluator Findings	The evaluator examined the section 9.4.4 titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that if the self test fails, the front panel LEDs blink and the TOE makes a clicking sound. The TOE disables the PSD switching functionality, and enters a disabled state. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.8.5 FPT_TST.1(2) TSS 4

Objective	The evaluator shall examine the TSS to verify that it describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.
Evaluator Findings	The evaluator examined the section 9.4.4 titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that the TOE can be rebooted to rerun the self test to clear the error. All errors are logged. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.8.6 FPT_TST.1(2) Guidance 1

Objective	The evaluators shall verify that the operational user guidance describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' section 4.2 of the [CC_Supp] provides instructions on how to initiate a self test, and how to exit self test mode. In the case of a failure, users are directed to contact Vertiv Technical Support. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.9 FPT_TST_EXT.1

5.5.9.1 FPT_TST_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.5.9.2 FPT_TST_EXT.1 TSS 1

Objective	The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.
Evaluator Findings	The evaluator examined the section 9.4.4 titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that the TOE front panel LEDs blink and there is a clicking noise made by the TOE when a self-test fails. The TOE disables the PSD switching functionality and remains in a disabled state until the TOE is rebooted and the self-test passes. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.9.3 FPT_TST_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance: a) describes how the results of self-tests are indicated to the user; b) provides the user with a clear indication of how to recognize a failed self-test; and c) details the appropriate actions to be completed in the event of a failed self-test.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' section 4.2 of the [CC_Supp] describes a self-test failure and explains what the operator has to do if there is a failure. The channel indicators on the front panel light up sequentially and peripheral port interfaces are disabled during the self-test and following a

	failed self-test. In the event of a failed self-test, users are directed to contact Veritv Technical Support. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.9.4 FPT_TST_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance provides adequate information on TOE self-test failures, their causes, and their indications.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' section 4.2 of the [CC_Supp] describes a self-test failure. The document indicates that self-test failures may be caused by an unexpected input at power up, or by a failure in the device integrity. Self-test failures are indicated by blinking LEDs. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.6 TSS, Isolation Document, and Guidance Activities (TOE Access)

5.6.1 FTA_CIN_EXT.1

5.6.1.1 FTA_CIN_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.6.1.2 FTA_CIN_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes how the TOE behaves on power up and on reset, if applicable, regarding which computer interfaces are active, if any.
Evaluator Findings	The evaluator examined the section 9.5 titled 'TOE Access' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that on power up or power up following reset, all peripherals are connected to channel #1, and the corresponding push button LED will be illuminated. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.6.1.3 FTA_CIN_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.

Evaluator Findings	The evaluator examined the section 9.5 titled 'TOE Access' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the switching functionality, including the 'Freeze USB' and 'Freeze Audio' functions which allow independent switching of these functions. The description and figure show how the selected channel is indicated and that no conflicting information is displayed. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.6.1.4 FTA_CIN_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance notes which computer connection is active on TOE power up or on recovery from reset, if applicable. If a reset option is available, use of this feature must be described in the operational user guidance.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the [CC_Supp] and the [Tech_Bull]. The 'Selected Channel at Startup' section 4.4 of the [CC_Supp] indicates that Channel 1 is selected by default when the device is started or reset. Reset is described in the [Tech_Bull] section 2.2.6. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.6.1.5 FTA_CIN_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the [2306], [2307], [2282], and [2284]. These guides describe the behavior of the TOE indicators in section 4 of [2306], [2307], [2282] and section 5 of [2284]. These documents provide a diagram and a description of the channel indicators and a description of the indicator behavior when the switching mechanism is in use. This behavior ensures that no conflicting information is displayed by the indicators. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

The TOE was tested with the remote control (where appropriate).

NOTE: Though not explicitly defined by any EAs in the PP/SD, additional testing has been performed to verify that the USB-C port on the DPHC model is video only and does not provide peripheral device connections.

6.1 FAU_GEN.1 Test 1

Item	*Data/Description*
Test ID	*FAU_GEN.1 – Test 1*
Objective	The evaluator shall perform each of the auditable functions to succeed, and where possible, to fail. The evaluator shall use the means described in the TSS to access the audit records and verify that each of the events has been recorded, with all the of the expected information.
Notes	• The following are all auditable events for SC945DPH, SCM185DPH, SC845DPHC and SCMV245DPH: 1) Tampering event log - The TOE does not provide an audit for a failure of this event log. The evidence provided in FAU_GEN.1 records a successful capture of a tampering event log. 2) Self-test failure log - The TOE does not provide an audit for a failure of this event log. The evidence provided in FAU_GEN.1 records a successful capture of a self-test failure event log. 3) Peripheral device rejection event log - The TOE provides both a success and failure audit log for a peripheral device acceptance or reject. The evidence provided in FAU_GEN.1 records a successful capture of a peripheral device rejection event log. 4) Reset to factory default event log - The TOE does not provide an audit for a failure of this event log. The evidence provided in FAU_GEN.1 records a successful capture of a reset to factory default event log. 5) Primary administrator password change event log - The TOE does not provide an audit for a failure of this event log. The evidence provided in FAU_GEN.1 records a successful capture of a primary administrator password change event log. 6) Peripheral device acceptance event log - The TOE provides both a success and failure audit log for a peripheral device acceptance or reject. The evidence provided in FAU_GEN.1 records a successful capture of a peripheral device acceptance event log. 7) Non-related configuration event log - The TOE does not provide an audit for a failure of this event log. The evidence provided in FAU_GEN.1 records a successful capture of a non-related configuration event log. 8) Administrator login event log - The TOE provides both a success and failure audit log for an administrator login or logout event. The evidence provided in FAU_GEN.1 records a successful capture of an administrator login event log. 9) Administrator logout event log - The TOE provides both a success and failure audit log for an administrator login or logout event. The evidence provided in FAU_GEN.1 records a successful capture of an administrator logout event log. 10) Creation of administrator account event log - The TOE does not provide an audit for a failure of this event log. The evidence provided in FAU_GEN.1

	records a successful capture of a creation of administrator account event log. 11) Removal of administrator account event log - The TOE does not provide an audit for a failure of this event log. The evidence provided in FAU_GEN.1 records a successful capture of a removal of administrator account event log. 12) Administrator password change event log - The TOE does not provide an audit for a failure of this event log. The evidence provided in FAU_GEN.1 records a successful capture of an administrator password change event log. 13) Password lock event log - The TOE does not provide an audit for a failure of this event log. The evidence provided in FAU_GEN.1 records a successful capture of a password lock event log. 14) Startup and shutdown of the audit function - The TOE initiates the startup and shutdown of all audit event functionality automatically and does not produce any audit events pertaining to such. The start and stop of the audit function is implied by the power-up event. 15) CDF list modification log – The TOE does not provide an audit for a failure of this log. The evidence provided records a successful DPP change event.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. Set up the TOE to enable administrator access per applicable TOE administrative guidance. Verify that the TOE is in factory default format. 2. Attempt to set the initial administrator username and password. 3. Log into the TOE using administrative credentials and password. 4. Under the main operation page, select option “6” then “1” for critical one-time programming (OTP) logs. 5. Ensure tampering events logs are recorded by the TOE. 6. Ensure self-test failure logs are recorded by the TOE. 7. Ensure peripheral device rejection logs are recorded by the TOE 8. Ensure whitelist/blacklist configuration change logs are recorded by the TOE. 9. Ensure reset to factory default event logs are recorded by the TOE. 10. Ensure changes to the primary administrator password logs are recorded by the TOE. 11. Under the main operations page, select option “6” then “2” for random access memory (RAM) logs. 12. Ensure peripheral device acceptance logs are recorded by the TOE. 13. Ensure non-security related configuration change logs are recorded by the TOE. 14. Ensure administrator login logs are recorded by the TOE. 15. Ensure administrator logout logs are recorded by the TOE. 16. Ensure creation and removal of administrator account logs are recorded by the TOE. 17. Ensure administrator password change logs are recorded by the TOE. 18. Ensure password lock event logs are recorded by the TOE. 19. Ensure the power-up event log is recorded by the TOE
Expected Output	1. TOE is set to enable administrator access; TOE is in factory default format. 2. Initial administrator username and password is set. 3. Logged into the TOE using administrative credentials and password. 4. Critical one-time programming logs will be presented with different administrative function options.

	5. Tampering event logs will be recorded and present in the TOE logs. 6. Self-test failure logs will be recorded and present in the TOE logs. 7. Peripheral device rejection logs will be recorded and present in the TOE logs. 8. Whitelist/blacklist configuration change logs will be recorded and present in the TOE logs. 9. Reset to factory default event logs will be recorded and present in the TOE logs. 10. Changes to the primary administrator password logs will be recorded and present in the TOE logs. 11. Random access memory logs will be presented with different administrative function options. 12. Peripheral device acceptance logs will be recorded and present in the TOE logs. 13. Non-security related configuration change logs will be recorded and present in the TOE logs. 14. Administrator login logs will be recorded and present in the TOE logs. 15. Administrator logout logs will be recorded and present in the TOE logs. 16. Creation and removal of administrator account logs will be recorded and present in the TOE logs. 17. Administrator password change logs will be recorded and present in the TOE logs. 18. Password lock event logs will be recorded and present in the TOE logs. 19. Power-up event log will be recorded and present in the TOE logs.
Execution output	1. The TOE was set to enable administrator access through the administrator console window (Notepad). Option 5 was then selected to have the TOE reset to factory default format. 2. The Initial administrator username and password was set through the administrator console. 3. The evaluator logged into the TOE using administrative credentials and password. 4. Critical one-time programming logs were presented with different administrative function options. 5. The evaluator confirmed tampering event logs were recorded and present in the TOE logs. 6. The evaluator confirmed self-test failure logs were recorded and present in the TOE logs. 7. The evaluator confirmed peripheral device rejection logs were recorded and present in the TOE logs. 8. The evaluator confirmed that whitelist/blacklist configuration change logs were recorded and present in the TOE logs. 9. The evaluator confirmed reset to factory default event logs were recorded and present in the TOE logs. 10. The evaluator confirmed changes to the primary administrator password logs were recorded and present in the TOE logs. 11. Random access memory logs were presented with different administrative function options. 12. The evaluator confirmed peripheral device acceptance logs were recorded and present in the TOE logs. 13. The evaluator confirmed non-security related configuration change logs were recorded and present in the TOE logs.

	14. The evaluator confirmed administrator login logs were recorded and present in the TOE logs. 15. The evaluator confirmed administrator logout logs were recorded and present in the TOE logs. 16. The evaluator confirmed creation and removal of administrator account logs were recorded and present in the TOE logs. 17. The evaluator confirmed administrator password change logs were recorded and present in the TOE logs. 18. The evaluator confirmed password lock event logs were recorded and present in the TOE logs. 19. The evaluator confirmed that the power-up event was recorded and present in the TOE logs.			
Pass/Fail Explanation	The evaluator confirmed that each of the required auditable events has been recorded, with all the of the expected information.			
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS	PASS

6.2 FDP_AFL_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FDP_AFL_EXT.1 – Test 1*
Objective	Step 1: Connect a computer to the TOE analog audio output peripheral interface and run audio analyzer software on it. Step 2: For each connected computer, ensure it is selected, use its tone generator software to generate a sine wave audio tone for each of the frequencies in the Audio Filtration Specifications table and verify in the audio analyzer software that they are attenuated by at least the amount specified in the Audio Filtration Specifications table. Step 3: Connect an oscilloscope to the TOE analog audio output peripheral interface and set it to measure the peak-to-peak voltage. Step 4: For each connected computer, perform step 5 with the signal generator set to the following settings: • Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed • Signal average to 0V (negative swing) Step 5: Set the signal generator to generate the frequencies in Audio Filtration Specifications table and verify the signal on the oscilloscope does not exceed the corresponding maximum voltage after attenuation.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, TrueRTA, Rigol Waveform Audio Signal Generator, Tektronix Oscilloscope, Spliced 3.5mm Cable, Dell P2319H Monitor.
Test Execution Steps	1. Connect a computer to the TOE analog audio output peripheral interface and run audio analyzer software on it. 2. For each connected computer, ensure it is selected, use its tone generator software to generate a sine wave audio tone for each of the frequencies in the

	Audio Filtration Specifications table and verify in the audio analyzer software that they are attenuated by at least the amount specified in the Audio Filtration Specifications table. 3. Connect an oscilloscope to the TOE analog audio output peripheral interface and set it to measure the peak-to-peak voltage. 4. For each connected computer, perform step 5 with the signal generator set to the following settings: • Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed. • Signal average to 0V (negative swing). 5. Set the signal generator to generate the frequencies in Audio Filtration Specifications table and verify the signal on the oscilloscope does not exceed the corresponding maximum voltage after attenuation.		
Expected Output	1. Audio analyzer software running on computer connected to the TOE analog audio output peripheral interface. 2. Attenuation level is at least the amount specified in the Audio Filtration Specifications table. 3. Oscilloscope connected to the TOE analog output peripheral. 4. Connected audio signal generator. 5. Detected signal does not exceed the corresponding maximum voltage after attenuation.		
Execution Output	1. The evaluator connected a computer (LAB PC) to the TOE analog audio output peripheral interface port. The evaluator verified that the audio analyzer software was running on computer connected to the TOE analog audio output peripheral interface (LAB PC). 2. The evaluator verified that for each connected computer it was selected, and the tone generator software / hardware (Rigol) was used to generated a sine wave audio tone for each frequency. The evaluator verified that the attenuation level was at least the amount specified in the Audio Filtration Specifications table. 3. The evaluator verified that the Oscilloscope was connected to the TOE analog output peripheral and was set to measure the peak-to-peak voltage (Vpp). 4. The evaluator ensured that for each connected computer, step #5 was performed with the settings specified. 5. The evaluator set the signal generator to generate the frequencies in the audio filtration specifications table. The evaluator verified that the detected signal did not exceed the corresponding maximum voltage after attenuation.		
Pass/Fail Explanation	The evaluator confirms that the TOE audio function implementation properly filters the audio passing through the TOE. The frequencies are attenuated by at least the amount specified in the Audio Filtration Specifications table, and the oscilloscope does not exceed the corresponding maximum voltage after attenuation.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.3 FDP_APC_EXT.1 Test 1

Objective	There are no test Evaluation Activities for this component.

Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.4 FDP_APC_EXT.1/AO Test 1

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/AO – Test 1*
Objective	The evaluator shall perform the following setup steps: • Configure the TOE and the operational environment in accordance with the operational guidance. • Play a different audio file on a number of computers for each TOE computer analog audio interface. • Connect each computer to a TOE computer analog audio interface. • Turn on the TOE. Note that for a TOE that provides audio mixing function the evaluator shall maximize the volume on a specific channel where instructed in the following text to assign that specific computer. Note: Electrical signals are considered not to flow between connected computers and data is considered not to transit the TOE if no signal greater than 45 dB of attenuation at the specific audio frequency is received Test 1-AO – Analog Audio Output Data Routing Methods. This test verifies the functionality of the TOE routing methods while powered on, powered off, and in failure state. Step 1: Connect amplified speakers to the TOE audio output device interface. Set the speakers to approximately 25% volume. Step 2: [Conditional: if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP, then] perform step 3 for each switching method selected in FDP_SWI_EXT.2.2 in accordance with the operational user guidance. Step 3: For each connected computer, ensure it is selected, listen to the amplified speakers, and verify that the audio is coming from the selected computer(s). Adjust the volume if necessary. Step 4: Replace the speakers with a computer connected to the TOE analog audio output device interface and run audio spectrum analyzer software on it. Run tone generator software on all connected computers. Step 5: Turn off the TOE, and for each connected computer, use the tone generator program to generate a sine wave audio tone for each of the designated frequencies and verify that no audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface.

	Step 6: Power on the TOE, cause the TOE to enter a failure state, and verify that the TOE provides the user with an indication of failure. For each connected computer use the tone generator program to generate a sine wave audio tone for each of the designated frequencies and verify that no audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Edifier Multimedia Speaker, TrueRTA, Rigol Waveform Audio Signal Generator, Dell P2319H Monitor.
Test Execution Steps	1. Connect amplified speakers to the TOE audio output device interface. Set the speakers to approximately 25% volume. 2. *[Conditional: if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP, then]* perform step 3 for each switching method selected in FDP_SWI_EXT.2.2 in accordance with the operational user guidance. 3. For each connected computer, ensure it is selected, listen to the amplified speakers, and verify that the audio is coming from the selected computer(s). Adjust the volume if necessary. 4. Replace the speakers with a computer connected to the TOE analog audio output device interface and run audio spectrum analyzer software on it. Run tone generator software on all connected computers. 5. Turn off the TOE, and for each connected computer, use the tone generator program to generate a sine wave audio tone for each of the designated frequencies and verify that no audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface. 6. Power on the TOE, cause the TOE to enter a failure state, and verify that the TOE provides the user with an indication of failure. For each connected computer use the tone generator program to generate a sine wave audio tone for each of the designated frequencies and verify that no audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface.
Expected Output	1. Audio is audible. 2. Performing steps 3; "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP. 3. Audio is audible only from the selected computers. 4. Speakers replaced with audio spectrum analyzer and tone generator software running on all computers. 5. No Sound heard through the audio spectrum analyzer. 6. No sound heard through audio spectrum analyzer.
Execution Output	1. A speaker was connected to the TOE audio output interface. The evaluator set the speaker to approximately 25% volume. 2. Performed step 3 for both the front panel buttons and the remote control; "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP. 3. The evaluator ensured that for each connected computer it was selected. The audio was verified to be coming from the each connected computer successfully. The evaluator verified that when each computer was selected the correct accompanying audio was heard through the speaker. When the next computer was selected the previous computers audio was cut off and the

	evaluator was presented with the correct audio on the currently selected computer. 4. Speakers were replaced with audio spectrum analyzer. This consisted of a 3.5mm cable connected from the TOE analog audio output device interface port and connected to the LAB PC. Tone generator software was running on all connected computers. These were connected to the TOE by 3.5mm audio cables into the TOE corresponding audio input port for each computer. 5. The evaluator ensured the TOE was turned off. For each connected computer the tone generator software or hardware generator (Rigol) was used to generate each of the desired frequencies. No audio was present through the audio spectrum analyzer software connected to the TOE analog audio output device interface (LAB PC). 6. The evaluator ensured the TOE entered a failure state. This was visually confirmed by the front panel LED indicators cycling through all channels, and no operational functionality being present. For each connected computer the tone generator software or hardware generator (Rigol) was used to generate each of the desired frequencies. No audio was present through the audio spectrum analyzer software connected to the TOE analog audio output device interface (LAB PC).		
Pass/Fail Explanation	The functionality of the TOE's routing methods has been tested while powered on, powered off, and in failure state. The evaluator confirms that audio is only routed to selected authorized computers.		
Remote Control Used	SCAFP0004	SCAFP0004	SCAFP0004
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.5 FDP_APC_EXT.1/AO Test 2

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/AO – Test 2*
Objective	Test 2-AO – Analog Audio Output Interface Isolation [Conditional: perform this test if "switching through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.] This test verifies that no data or electrical signals flow between connected computers while the TOE is powered on or off. Step 1. Continue with the setup from Test 1. Step 2: Connect a computer to the TOE analog audio output device interface. Run audio spectrum analyzer software on all computers. Step 3: Perform steps 4-13 for each TOE analog audio computer interface. Step 4: Turn on the TOE and ensure the first computer is selected. Step 5: Use the tone generator program on the first computer to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface and is not present in the audio spectrum analyzer software on any of the non-selected computers. This step does not fail if

	frequencies above 20 kHz are not present in the software on the connected computer due to attenuation as per FDP_AFL_EXT.1 Step 6: For each other TOE analog audio computer interface, select that computer and use the tone generator program on the first computer (now no longer selected) to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is not present in the audio spectrum analyzer software on the selected computer, the other non-selected computers, or the computer connected to the TOE analog audio output device interface. Step 7: Power off the TOE and use the tone generator program on the first computer to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is not present in the audio spectrum analyzer software on any of the other connected computers. Step 8: Restart the TOE, select the first computer, and replace it with an external audio signal generator. Step 9: For each non-selected computer connected to the TOE analog audio output computer interface, replace it with an oscilloscope set to measure the peak-to-peak voltage and perform steps 10-14. Step 10: Perform steps 11-13 with the signal generator set to the following settings: Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed Signal average to 0v (negative swing) Step 11: Set the signal generator to generate the designated frequencies and verify the signal on the oscilloscopes is 11.2 mV or less. This level of signal ensures signal attenuation of 45 dB in the extended audio frequency range. Step 12: For each other TOE analog audio computer interface, select it, set the signal generator to generate the designated frequencies, and verify the signal on the oscilloscopes is 11.2 mV or less. Step 13: Power off the TOE and set the signal generator to generate the designated frequencies and verify the signal on the oscilloscopes is 11.2 mV or less.
Notes	• TD0585 applied.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, TrueRTA, Rigol Waveform Audio Signal Generator, Tektronix Oscilloscope, Dell P2319H Monitor, Spliced 3.5mm Cable.
Test Execution Steps	1. Continue with the setup from Test 1. 2. Connect a computer to the TOE analog audio output device interface. Run audio spectrum analyzer software on all computers. 3. Perform steps 4-13 for each TOE analog audio computer interface. 4. Turn on the TOE and ensure the first computer is selected. 5. Use the tone generator program on the first computer to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is present in the audio spectrum analyzer software on the computer connected to the TOE analog audio output device interface and is not present in the audio spectrum analyzer software on any of the non-selected computers. 6. For each other TOE analog audio computer interface, select that computer and use the tone generator program on the first computer (now no longer selected)

	to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is not present in the audio spectrum analyzer software on the selected computer, the other non-selected computers, or the computer connected to the TOE analog audio output device interface. 7. Power off the TOE and use the tone generator program on the first computer to generate a sine wave audio tone for each of the designated frequencies. Verify that the audio is not present in the audio spectrum analyzer software on any of the other connected computers. 8. Restart the TOE, select the first computer, and replace it with an external audio signal generator. 9. For each non-selected computer connected to the TOE analog audio output computer interface, replace it with an oscilloscope set to measure the peak-to-peak voltage and perform steps 10-14. 10. Perform steps 11-13 with the signal generator set to the following settings: Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed Signal average to 0v (negative swing). 11. Set the signal generator to generate the designated frequencies and verify the signal on the oscilloscopes is 11.2 mV or less. This level of signal ensures signal attenuation of 45 dB in the extended audio frequency range. 12. For each other TOE analog audio computer interface, select it, set the signal generator to generate the designated frequencies, and verify the signal on the oscilloscopes is 11.2 mV or less. 13. Power off the TOE and set the signal generator to generate the designated frequencies and verify the signal on the oscilloscopes is 11.2 mV or less.
Execution Output	1. The evaluator continued with same test setup from Test 1 (FDP_APC_EXT.1 – Test 1). 2. The evaluator connected the LAB PC to the TOE analog audio output device interface with a 3.5mm audio cable. Audio spectrum analyzer software was running on all computers. 3. The evaluator ensured steps 4-13 were performed for each TOE analog audio computer interface. 4. The evaluator ensured the TOE was powered on and computer #1 was selected. 5. The evaluator used the tone generator program or hardware generator (Rigol) to generate a sine wave audio for each of the designated frequencies. The evaluator verified that the audio was present in the audio spectrum analzyer software connected to the TOE analog output device interface port (LAB PC). When the evaluator produced said frequency a noticeable increase in audio was present on the audio spectrum software (LAB PC). When the evaluator discontinued generating the sine wave audio the audio present diminished and was no longer detectable. The evaluator verified that no audio was present on the non-selected computers audio spectrum analzer software (PC #2). 6. For each other TOE analog audio computer interface the evaluator selected that computer and used the tone generator software/hardware on the first computer – PC #1 (which was now no longer the selected computer) and generated a sine wave audio tone for each of the designated frequencies. The evaluator verified that no audio was present on the audio spectrum analyzer on non-selected computers (PC #2), or the the computer connected to the TOE analog audio output device interface (LAB PC).

	7. The evaluator powered off the TOE and used the tone generator program/hardware on the first computer (PC#1) to generate a sine wave audio tone for each of the designated frequencies. No audio was present on audio spectrum analyzer on other connected computers. 8. The evaluator restarted the TOE. The first computer was replaced with an external audio signal generator (Rigol). 9. The evaluator ensured that for each non-selected computer connected to the TOE analog audio output computer interface, it was replaced with an oscilloscope. The oscilloscope was set to measue the peak-to-peak voltage needed to perform steps 10 – 14. 10. The evaluator performed steps 11- 13 with the Signal generator signal being set to 2.00 V peak-to-peak, calibrating the signal as needed Signal average to 0v. 11. The evaluator set the signal generator to generate the desired frequencies and verified that the signal on the oscilloscope was 11.2 mV or less. 12. The evaluator selected each other TOE analog audio computer interface and set the signal generator to generate the desired frequencies. The evaluator verified the signal on the oscilloscope was 11.2 mV or less. 13. The evaluator powered off the TOE and set the signal generator to generate the desired frequencies. The evaluator verified the signal on the oscilloscope was 11.2 mV or less.		
Pass/Fail Explanation	No data or electrical signals flow between connected computers while the TOE is powered on or off. The evaluator has confirmed that audio is only present on the selected computer and does not leak to other connected computers.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.6 FDP_APC_EXT.1/AO Test 3

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/AO – Test 3*
Objective	Test 3-AO – No Flow between Computers with Other Peripheral Device Types [Conditional: Perform this test only if a PP-Module aside from the Analog Audio Output PP-Module is part of the PP-Configuration being claimed AND if "switching through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.] This test verifies that power events at one TOE USB computer interface do not affect the analog audio output computer interface of another computer. Note: "No sound appears" is defined as a temporary jump of at least 4 dB from the existing ambient noise floor. Step 1: Connect a computer to the TOE analog audio output peripheral interface and run audio spectrum analyzer software on it and each connected computer. Step 2: Perform steps 3-9 for each connected computer. Step 3: Ensure the first computer is selected and perform steps 4-8 while the TOE is powered on and powered off. [Conditional: Perform steps 4 and 5 only if the PP-Module for Video/Display Devices is part of the PP Configuration being claimed.]

	Step 4: For each other connected computer, disconnect and reconnect the video cables from the TOE computer interface several times. Verify that no sound appears on the audio analyzer software on the first computer. Step 5: Disconnect and reconnect the first computer's video cables from the TOE computer interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers. Step 6: [Conditional: If the PP-Module for Keyboard/Mouse Devices or PP-Module for User Authentication Devices is part of the PP-Configuration being claimed, then:] for each other connected computer, disconnect and reconnect the USB cable from the TOE USB computer interface several times. Verify that no sound appears on the audio analyzer software on the computer connected to the TOE analog audio output peripheral interface or any connected computers. Step 7: [Conditional: If the PSD PP-Module for Keyboard/Mouse Devices is part of the PP-Configuration being claimed, then:] disconnect and reconnect the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM from the TOE KM peripheral device interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers. Step 8: [Conditional: If the PP-Module for User Authentication Devices is part of the PP-Configuration being claimed and "external" is selected in FDP_PDC_EXT.4.1, then:] disconnect and reconnect the UA peripheral device from the TOE UA peripheral device interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers. Step 9: [Conditional: If the PP-Module for User Authentication Devices is part of the PP-Configuration being claimed, then:] connect an authentication session to the first computer and verify that no sounds appears on the audio analyzer software on the other connected computers.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, TrueRTA, Rigol Waveform Audio Signal Generator, Dell P2319H Monitor.
Test Execution Steps	1. Connect a computer to the TOE analog audio output peripheral interface and run audio spectrum analyzer software on it and each connected computer. 2. Perform steps 3-9 for each connected computer. 3. Ensure the first computer is selected and perform steps 4-8 while the TOE is powered on and powered off. 4. For each other connected computer, disconnect and reconnect the video cables from the TOE computer interface several times. Verify that no sound appears on the audio analyzer software on the first computer. 5. Disconnect and reconnect the first computer's video cables from the TOE computer interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers. 6. *[Conditional: If the PP-Module for Keyboard/Mouse Devices or PP-Module for User Authentication Devices is part of the PP-Configuration being claimed, then:]* for each other connected computer, disconnect and reconnect the USB cable from the TOE USB computer interface several times. Verify that no sound appears on the audio analyzer software on the computer connected to the TOE analog audio output peripheral interface or any connected computers.

	7. *[Conditional: If the PSD PP-Module for Keyboard/Mouse Devices is part of the PP-Configuration being claimed, then:]* disconnect and reconnect the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM from the TOE KM peripheral device interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers. 8. *[Conditional]: If the PP-Module for User Authentication Devices is part of the PP-Configuration being claimed and "external" is selected in FDP_PDC_EXT.4.1, then:]* disconnect and reconnect the UA peripheral device from the TOE UA peripheral device interface several times. Verify that no sound appears on the audio analyzer software on the other connected computers. 9. *[Conditional: If the PP-Module for User Authentication Devices is part of the PP-Configuration being claimed, then:]* connect an authentication session to the first computer and verify that no sounds appears on the audio analyzer software on the other connected computers.		
Execution Output	1. The evaluator connected the LAB PC with a 3.5mm audio cable to the TOE analog audio output peripheral interface port. Audio spectrum analyzer software was running on the LAB PC and each connected computer (PC #1 & PC #2). 2. The evaluator performed steps 3 - 9 on each connected computer. 3. The evaluator performed steps 4 - 8 while TOE was powered on and powered off. 4. The evaluator disconnected and reconnected the video cables from the TOE computer interface several times for the computer #2 connection. The evaluator verified that no sound appeared on audio analyzer software on first computer (PC #1). 5. The evaluator disconnected and reconnected the first computer (PC #1) video cables from the TOE computer interface several times. The evaluator verified that no sound appeared on audio analyzer software on the other connected computers (PC #2). 6. For each other connected computer, the evaluator disconnected and reconnected the USB cable from the TOE USB computer interface several times. The evaluator verified that no sound appeared on the audio analyzer software on the TOE analog audio output peripheral interface (LAB PC) or any connected computers. 7. The evaluator disconnected and reconnected the TOE KM peripheral device interface several times. The evaluator verified that no sound appeared on the audio analyzer software on other connected computers (PC #1 or PC #2). 8. The evaluator disconnected and then reconnected the UA peripheral device from the TOE UA peripheral device interface several times. The evaluator verified that no sound appeared on the audio analyzer software on other connected computers (PC #1 or PC #2). 9. The evaluator connected an authentication session to the first computer (PC #1) and verified that no sounds appeared on other connected computers (PC #2).		
Pass/Fail Explanation	The evaluator has confirmed that power events at one TOE USB computer interface do not affect the analog audio output computer interface of another computer.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.7 FDP_APC_EXT.1/AO Test 4

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/AO – Test 4*
Objective	Test 4-AO – No Flow between Connected Computers over Time This test verifies that the TOE does not send data to different computers connected to the same interface at different times. Repeat this test for each TOE Analog Audio Output port. Step 1: Ensure only one computer is connected and it is selected. Run a tone generator program on the connected computer and the audio analyzer software on a non-connected computer. Step 2: Perform steps 3-11 while the TOE is powered on and powered off. Step 3: Perform steps 4-5 for each of the designated frequencies. Step 4: Use the tone generator program on the connected computer to generate a sine wave audio tone. Step 5: Disconnect the connected computer, wait two minutes, connect the other computer, and verify that the generated audio frequency is not present in the audio spectrum analyzer software. Step 6: Replace the connected computer with an external audio signal generator. Step 7: Perform steps 8-11 with the signal generator set to the following settings: Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed Signal average to 0v (negative swing) Step 8: Perform steps 9-11 for each of the designated frequencies. Step 9: Use the signal generator to generate the signal. Step 10: Disconnect the signal generator, wait two minutes, and replace it with an oscilloscope set to measure the peak-to-peak voltage. Step 11: Verify the signal on the oscilloscope is 11.2 mV or less at the generated frequency.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, TrueRTA, Rigol Waveform Audio Signal Generator, Tektronix Oscilloscope, Dell P2319H Monitor, Spliced 3.5mm Cable.
Test Execution Steps	1. Ensure only one computer is connected and it is selected. Run a tone generator program on the connected computer and the audio analyzer software on a non-connected computer. 2. Perform steps 3-11 while the TOE is powered on and powered off. 3. Perform steps 4 - 5 for each of the designated frequencies. 4. Use the tone generator program on the connected computer to generate a sine wave audio tone. 5. Disconnect the connected computer, wait two minutes, connect the other computer, and verify that the generated audio frequency is not present in the audio spectrum analyzer software. 6. Replace the connected computer with an external audio signal generator.

	7. Perform steps 8-11 with the signal generator set to the following settings: 11 Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed Signal average to 0v (negative swing). 8. Perform steps 9 - 11 for each of the designated frequencies. 9. Use the signal generator to generate the signal. 10. Disconnect the signal generator, wait two minutes, and replace it with an oscilloscope set to measure the peak-to-peak voltage. 11. Verify the signal on the oscilloscope is 11.2 mV or less at the generated frequency.		
Execution Output	1. The evaluator ensured only one computer is connected and it is selected (PC #1). The evaluator verified that the tone generator was running on connected computer (PC #1) and audio analyzer software on a non-connected computer (PC #2). 2. The evaluator verified that steps 3 - 11 were performed while the TOE was powered on and powered off. 3. The evaluator verified that steps 4 - 5 were performed for each designated frequency. 4. The evaluator used the tone generator program or tone generator hardware (Rigol) to generate a sine wave audio tone. 5. The evaluator disconnected the connected computer (#1) or tone generator hardware (Rigol), waited two minutes, and connected the other computer (PC #2). The evaluator verified that no audio frequencies were present in the audio spectrum analyzer software (PC #2). 6. The evaluated replaced the computer with an external audio signal generator (Rigol). 7. The evaluator connected the audio signal generator and set 0V (negative swing) and 2V peak-to-peak output signal. 8. The evaluator performed steps 9 – 11 for each designated frequency. 9. The evaluator verified that the signal was generated. 10. The evaluator disconnected the signal generator, waited two minutes, and replaces it with an Oscilloscope set to measure peak-to-peak voltage. 11. The evaluator verified that the signal on the oscilloscope was 11.2 mV or less at the generated frequency.		
Pass/Fail Explanation	The evaluator verified that the TOE does not send data to different computers connected to the same interface at different times and the signal was 11.2mV or less at the generated frequency.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.8 FDP_APC_EXT.1/KM Test 1

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/KM – Test 1*
Objective	For tests that use the USB sniffer or USB analyzer software, the evaluator verifies whether traffic is sent or not sent by inspection of the passing USB transactions and ensuring they do not contain USB data payloads other than any expected traffic, as well as USB NAK transactions or system messages. To avoid clutter

	during USB traffic capture, the evaluator may filter NAK transactions and system messages. The evaluator shall perform the following tests: Test 1-KM – KM Switching methods [Conditional: Perform this test if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP] While performing this test, ensure that switching is always initiated through express user action. This test verifies the functionality of the TOE’s KM switching methods. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Run an instance of a text editor on each connected computer. Step 2: Connect a display to each computer in order to see all computers at the same time, turn on the TOE, and enter text or move the cursor to verify which connected computer is selected. Step 3: For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational user guidance, and verify that it succeeds. Step 4: For each peripheral device type selected in FDP_PDC_EXT.3.1/KM, attempt to switch the device to more than one computer at once and verify that the TOE ignores all such commands or otherwise prevents the operation from executing. Step 5: [Conditional: If “keyboard” is selected in FDP_PDC_EXT.3.1/KM, then] attempt to control the computer selection using the following standard keyboard shortcuts, where ‘#’ represents a computer channel number, and verify that the selected computer is not switched: • Control - Control - # - Enter • Shift - Shift - # • Num Lock - Minus - # • Scroll Lock - Scroll Lock - # • Scroll Lock - Scroll Lock - Function # • Scroll Lock - Scroll Lock - arrow (up or down) • Scroll Lock - Scroll Lock - # - enter • Control - Shift - Alt - # - Enter • Alt - Control - Shift - # Step 6: [Conditional: If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then] attempt to switch to other connected computers using the pointing device and verify that it does not succeed.

	Step 7: [Conditional: If “peripheral devices using a guard” is selected in FDP_SWI_EXT.2.2, then] attempt to switch to other connected computers using the peripheral device and guard by only performing some of the steps outlined in the operational user guidance, and verify that it does not succeed.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, Dell P2319H Monitor.
Test Execution Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Run an instance of a text editor on each connected computer. 2. Connect a display to each computer in order to see all computers at the same time, turn on the TOE, and enter text or move the cursor to verify which connected computer is selected. 3. For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational user guidance, and verify that it succeeds. 4. For each peripheral device type selected in FDP_PDC_EXT.3.1/KM, attempt to switch the device to more than one computer at once and verify that the TOE ignores all such commands or otherwise prevents the operation from executing. 5. *[Conditional: If “keyboard” is selected in FDP_PDC_EXT.3.1/KM, then]* attempt to control the computer selection using the following standard keyboard shortcuts, where ‘#’ represents a computer channel number, and verify that the selected computer is not switched: • Control - Control - # - Enter • Shift - Shift - # • Num Lock - Minus - # • Scroll Lock - Scroll Lock - # • Scroll Lock - Scroll Lock - Function # • Scroll Lock - Scroll Lock - arrow (up or down) • Scroll Lock - Scroll Lock - # - enter • Control - Shift - Alt - # - Enter • Alt - Control - Shift - # 6. *[Conditional: If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then]* attempt to switch to other connected computers using the pointing device and verify that it does not succeed. 7. *[Conditional: If “peripheral devices using a guard” is selected in FDP_SWI_EXT.2.2, then]* attempt to switch to other connected computers using the peripheral device and guard by only performing some of the steps outlined in the operational user guidance, and verify that it does not succeed.
Execution Output	1. The TOE was configured in accordance with the operational guidance. Authorized peripheral devices were connected to the TOE and a text editor was running on each connected computer. 2. The evaluator connected a display to each connected computer to see each computer at the same time. The TOE was powered on and the evaluator was able to verify which connected computer was selected. 3. The evaluator was able to switch between selected computers for each switching method selected in FDP_SWI_EXT.2.2. 4. The TOE prevented the evaluator from switching to more than one computer at once. The evaluator verified that the TOE ignored all such commands.

	5. The evaluator attempted to control the computer selection using the standard keyboard shortcuts. The TOE did not respond to such standard keyboard shortcuts. 6. The evaluator was not able to switch between computers using the pointing device and verifies it does not succeed. 7. "Peripheral devices using a guard" was not selected in FDP_SWI_EXT.2.2(1), therefore this test is only applicable to the SCMV245DPH. The evaluator attempted to perform only some of the required actions (e.g. Left Control, Left Control, Q) and found that switching did not occur until the full sequence of events was followed (Left Control, Left Control, Q + Left Control, Left Control O + Left Control, Left Control, F).		
Pass/Fail Explanation	The functionality of the TOE's KM switching methods has been tested successfully. The evaluator has confirmed that the TOE prevents the user from switching between more than one computer at once.		
Remote Control Used	SCAFP0004	SCAFP0004	SCAFP0004
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.9 FDP_APC_EXT.1/KM Test 2

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/KM – Test 2*
Objective	Test 2-KM – Positive and Negative Keyboard and Mouse Data Flow Rules Testing This test verifies the functionality for correct data flows of a mouse and keyboard during different power states of the selected computer. Step 1: Continue with the test setup from Test 1 and for each connected computer, connect a USB sniffer between it and the TOE or open the USB analyzer software. Perform steps 2-12 with each connected computer as the selected computer. Step 2: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer. [Conditional: Perform steps 3-10 if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.] Step 3: [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] switch the TOE to each connected computer, and use the mouse to position the mouse cursor at the center of each display. Switch the TOE back to the originally selected computer. Step 4: [If "keyboard is selected in FDP_PDC_EXT.3.1/KM, then] use the keyboard to enter text into the text editor. [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] use the mouse to move the cursor to the bottom right corner of the display. Step 5: Switch to each connected computer and verify that the actions taken in Step 4 did not occur on any of the non-selected computers. Step 6: Switch to the originally selected computer. Continue exercising the functions of the peripheral device(s) and examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent.

	Step 7: Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. Step 8: Reboot the selected computer. Examine the USB protocol analyzers on each one of the nonselected computers and verify that no traffic is sent. Step 9: Enter sleep or suspend mode in the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers to verify that no traffic is sent. Step 10: Exit sleep or suspend mode on the selected computer. Examine the USB protocol analyzers on each of the non-selected computers to verify that no traffic is sent. Ensure that any text in the Text Editor application is deleted. Step 11: Perform step 12 when the TOE is off and then in a failure state. Step 12: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that no results are observed on the selected computer and that no traffic is captured using the USB analyzer.
Test Equipment Used	Teledyne Lecroy USB sniffer, USBlyzer, Notepad, Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Execution Steps	1. Continue with the test setup from Test 1 and for each connected computer, connect a USB sniffer between it and the TOE or open the USB analyzer software. Perform steps 2-12 with each connected computer as the selected computer. 2. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer. 3. *[Conditional: Perform steps 3-10 if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.]* [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] switch the TOE to each connected computer and use the mouse to position the mouse cursor at the center of each display. Switch the TOE back to the originally selected computer. 4. [If "keyboard is selected in FDP_PDC_EXT.3.1/KM, then] use the keyboard to enter text into the text editor. [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] use the mouse to move the cursor to the bottom right corner of the display. 5. Switch to each connected computer and verify that the actions taken in Step 4 did not occur on any of the non-selected computers. 6. Switch to the originally selected computer. Continue exercising the functions of the peripheral device(s) and examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. 7. Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. 8. Reboot the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. 9. Enter sleep or suspend mode in the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers to verify that no traffic is sent.

	10. Exit sleep or suspend mode on the selected computer. Examine the USB protocol analyzers on each of the non-selected computers to verify that no traffic is sent. Ensure that any text in the Text Editor application is deleted. 11. Perform step 12 when the TOE is off and then in a failure state. 12. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that no results are observed on the selected computer and that no traffic is captured using the USB analyzer.		
Execution Output	1. The evaluator continued with the test setup from Test 1. USB analyzer software was running on each connected computer. 2. The evaluator exercised the functions of the peripheral device and observed the corresponding USB traffic being generated on the selected computer. 3. The evaluator placed the mouse cursor in the center of the display for each connected computer. 4. The evaluator used the keyboard to enter text into the text editor. Then mouse curser was placed in the bottom right corner of the display. 5. The evaluator confirms that the actions taken in step 4 did not occur on any of the non-selected computers. 6. The evaluator confirms no USB traffic was seen on the non-selected computers. This is confirmed by examining the USB analyzer on each non-selected computer and verifying no traffic is sent/captured. 7. No USB traffic was seen on the non-selected computers. This is confirmed by examining the USB analyzer on each non-selected computer and verifying no traffic is sent/captured. 8. No USB traffic was seen on the non-selected computers. This is confirmed by examining the USB analyzer on each non-selected computer and verifying no traffic is sent/captured. 9. No USB traffic was seen on the non-selected computers. This is confirmed by examining the USB analyzer on each non-selected computer and verifying no traffic is sent/captured. 10. No USB traffic was seen on the non-selected computers. This is confirmed by examining the USB analyzer on each non-selected computer and verifying no traffic is sent/captured. The Text in editor was then deleted. 11. The evaluator performed step 12 while the TOE was powered off, then again while in a failure state. No USB traffic was seen on the non-selected and selected computers. This is confirmed by examining the USB analyzer on each computer and verifying no traffic is sent/captured.		
Pass/Fail Explanation	Correct data flows of a mouse and keyboard during different power states of the selected computer has been tested. The evaluator has confirmed that data flow is transmitted to the correct computers at the accurate times. The expected USB traffic was observed on the selected computer and no traffic was observed when in a powered off state and during a failure state. The expected KM input was shown on the currently selected computer and not shown on non-selected computers. No output was observed on non-selected computers while rebooting, suspending or putting the selected computer to sleep.		
Remote Control Used	SCAFP0004	SCAFP0004	SCAFP0004
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.10 FDP_APC_EXT.1/KM Test 3

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/KM – Test 3*
Objective	Test 3-KM – Flow Isolation and Unidirectional Rule This test verifies that the TOE properly enforces unidirectional flow and isolation. Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Perform steps 2-12 with each connected computer as the selected computer. Step 2: Ensure the TOE is powered on and connect a display directly to the selected computer. Open a real-time hardware information console on the selected computer. [If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then perform steps 3-4] Step 3: Connect a gaming mouse with programmable LEDs directly to the selected computer and attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs change state. Step 4: Disconnect the gaming mouse from the selected computer and connect it to the TOE mouse peripheral device port through the USB sniffer. Attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs do not change state and that no traffic is sent and captured by the USB sniffer while the evaluator is not moving the mouse. [If “keyboard” is selected in FDP_PDC_EXT.3.1/KM, then perform step 5] Step 5: Connect a keyboard to the peripheral device interface through the USB sniffer. Use a keyboard emulation software application running on the selected computer to turn the keyboard Num Lock, Caps Lock, and Scroll Lock LEDs on and off. Verify that the LEDs on the keyboard do not change state and that no traffic is sent and captured by the USB sniffer. Step 6: Power down the TOE and disconnect the peripheral interface USB cable from the TOE to the selected computer and the peripheral devices from the TOE. Step 7: Power up the TOE and ensure the selected computer has not changed (this should have no effect on the selected computer because it was disconnected in the previous step). Reconnect the peripheral devices disconnected in step 6 to the TOE. Step 8: [If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the mouse LEDs are illuminated (indicating that the peripheral devices are powered on, although the selected computer is not connected). [If “keyboard” is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the Num Lock, Caps Lock, and Scroll Lock keyboard LEDs are blinking momentarily and then stay off (indicating that the keyboard is powered on, although the selected computer is not connected).

	Step 9: Turn the TOE off and disconnect the peripheral devices connected in step 6. Step 10: Reconnect the first computer interface USB cable to the TOE. Step 11: Turn on the TOE and check the computer real-time hardware information console for the presence of the peripheral devices connected in step 6 and disconnected in step 9. The presence of the TOE peripheral devices in the information console when the peripheral devices are not connected to the TOE indicates that the TOE emulates the KM devices. Step 12: [Conditional] If the TOE keyboard and mouse do not appear in the listed devices, repeat the following steps for both mouse and keyboard to simulate USB traffic: • Connect a USB generator to the TOE peripheral device interface port. • Configure the USB generator to enumerate as a generic HID mouse/keyboard device and then to generate a random stream of mouse/keyboard report packets. • Connect a USB sniffer device between the TOE computer interface and the USB port on the first computer to capture the USB traffic between the TOE and the first computer. Turn on the TOE and verify that no packets cross the TOE following the device enumeration.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Device Manager, Steelseries Rival 100 Gaming Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Execution Steps	1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. 2. Ensure the TOE is powered on and connect a display directly to the selected computer. Open a real-time hardware information console on the selected computer. 3. Connect a gaming mouse with programmable LEDs directly to the selected computer and attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs change state. 4. Disconnect the gaming mouse from the selected computer and connect it to the TOE mouse peripheral device port through the USB sniffer. Attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs do not change state and that no traffic is sent and captured by the USB sniffer while the evaluator is not moving the mouse. 5. Connect a keyboard to the peripheral device interface through the USB sniffer. Use a keyboard emulation software application running on the selected computer to turn the keyboard Num Lock, Caps Lock, and Scroll Lock LEDs on and off. Verify that the LEDs on the keyboard do not change state and that no traffic is sent and captured by the USB sniffer. 6. Power down the TOE and disconnect the peripheral interface USB cable from the TOE to the selected computer and the peripheral devices from the TOE. 7. Power up the TOE and ensure the selected computer has not changed (this should have no effect on the selected computer because it was disconnected

	in the previous step). Reconnect the peripheral devices disconnected in step 6 to the TOE. 8. [If "mouse" is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the mouse LEDs are illuminated (indicating that the peripheral devices are powered on, although the selected computer is not connected). [If "keyboard" is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the Num Lock, Caps Lock, and Scroll Lock keyboard LEDs are blinking momentarily and then stay off (indicating that the keyboard is powered on, although the selected computer is not connected). 9. Turn the TOE off and disconnect the peripheral devices connected in step 6. 10. Reconnect the first computer interface USB cable to the TOE. 11. Turn on the TOE and check the computer real-time hardware information console for the presence of the peripheral devices connected in step 6 and disconnected in step 9. The presence of the TOE peripheral devices in the information console when the peripheral devices are not connected to the TOE indicates that the TOE emulates the KM devices. 12. *[Conditional]* If the TOE keyboard and mouse do not appear in the listed devices, repeat the following steps for both mouse and keyboard to simulate USB traffic: • Connect a USB generator to the TOE peripheral device interface port. • Configure the USB generator to enumerate as a generic HID mouse/keyboard device and then to generate a random stream of mouse/keyboard report packets. • Connect a USB sniffer device between the TOE computer interface and the USB port on the first computer to capture the USB traffic between the TOE and the first computer. • Turn on the TOE and verify that no packets cross the TOE following the device enumeration.
Execution Output	1. The evaluator configured the TOE and operational environment in accordance with the operation guidance. 2. The TOE was powered on; each selected computer had display connected directly to them. The hardware information console was open on the selected computer. 3. The evaluator connected a gaming mouse with programmable LEDs directly to the selected computer and attempted to configure the LEDs using the appropriate mouse application. The mouse programmable LED did change state successfully. 4. The evaluator connected the gaming mouse to the TOE mouse peripheral device port through the USB sniffer. An attempt was made to configure the mouse programmable LEDs, but the programmable LEDs did not change state. No USB traffic was generated, and no traffic was sent or captured while the evaluator is not moving the mouse. 5. The evaluator connected a keyboard to the peripheral device interface through the USB sniffer. Keyboard LEDs do not change state as the TOE does not contain LEDs for Num Lock, Caps Lock or Scroll Lock. No USB traffic was sent and captured by the USB sniffer. 6. The evaluator ensured the TOE was powered off. The peripheral interface USB cable was unplugged.

	7. The evaluator powered on the TOE and verified the selected computer had not changed. The peripheral cable was reconnected. 8. Immediately following a mouse connection, the evaluator verifies that mouse LEDs are illuminated. For a keyboard connection the keyboard LEDs blinked momentarily then stayed off. 9. The evaluator ensured the TOE was powered off and the peripherals were disconnected. 10. The first computers USB cable was reconnected to the TOE. 11. The evaluator verified that hardware management console indicated emulated peripheral devices. 12. Keyboard and mouse did appear in the listed devices.		
Pass/Fail Explanation	Unidirectional flow and isolation of USB traffic has been tested. The evaluator has confirmed that USB traffic is enforced properly and in a single direction. This was tested on all four connected computers. Mouse LEDs are illuminated when expected, and change state only when not attached to a USB analyzer. Keyboard LEDs blink momentarily when connected and do not change state when attached to an analyzer. The devices were properly emulated by the TOE and no packets were captured following enumeration.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.11 FDP_APC_EXT.1/KM Test 4

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/KM – Test 4*
Objective	*[Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP]* This test verifies that no data flows between computer Interfaces while the TOE is powered on or powered off.
Notes	• TD0507 applied.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, USBlyzer, HSL USB Dummy Load, Dr. Meter DC Power Supply, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor, Spliced USB Type-A Cable.
Test Execution Steps	1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Connect a display directly to each connected computer. Perform steps 2-10 for each connected computer. 2. Connect a USB sniffer between a non-selected TOE KM computer interface and its computer. Run USB protocol analyzer software on all remaining computers. 3. Turn on the TOE and observe the TOE enumeration data flow in the protocol analyzer connected to the selected computer and is not in any other USB protocol analyzers or the USB sniffer. 4. Ensure the TOE is switched to the first computer. 5. Reboot the first computer. Verify that no USB traffic is captured on all non-selected computer USB protocol analyzers. 6. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers. 7. Perform steps 8 and 9 for each TOE keyboard/mouse peripheral interface.

	8. Connect a USB dummy load into the TOE KM peripheral device interface. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers. Remove the plug after the step is completed. 9. Connect a switchable 5-volt power supply with any compatible USB plug into the TOE KM peripheral device interface. Modulate the 5-volt supply (i.e., cycle on and off) manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on all non-selected computer USB analyzers. 10. Turn off the TOE. Verify that no new traffic is captured.		
Execution Output	1. The evaluator ensured the TOE and the operational environment was configured in accordance with the operation guidance. A display was connected to each computer. 2. The evaluator connected a USB sniffer between a non-selected TOE KM computer interface and its computer. USB analyzer software was running on all remaining computers. 3. The evaluator confirms TOE enumeration traffic was only being captured on the selected computer. No other data was captured on any other USB protocol analyzer or the USB sniffer. 4. The evaluator ensures only the first computer was selected. 5. The evaluator rebooted the first computer. No USB traffic was captured on all non-selected computers. 6. The evaluator generated intense HID traffic; however, no USB traffic was captured on all non-selected computers. 7. The evaluator performed steps 8 and 9 for each KM interface. 8. The evaluator connected a USB dummy load into the KM peripheral device interface. No USB traffic was captured on all non-selected computers. 9. The evaluator connected a switchable 5-volt power supply into the TOE KM peripheral device interface. No USB traffic was captured on all non-selected computers. The evaluator turned off the TOE. No USB traffic was captured on all non-selected computers.		
Pass/Fail Explanation	Correct data flow while the TOE is powered on or powered off has been tested. The evaluator confirmed that USB traffic is only captured on selected authorized computers.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.12 FDP_APC_EXT.1/KM Test 5

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/KM – Test 5*
Objective	Test 5-KM – No Flow between Connected Computers over Time This test verifies that the TOE does not send data to different computers connected to the same interface at different times. Repeat this test for each TOE KM computer port. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in

	FDP_PDC_EXT.3.1/KM. Connect two computers to a different display and run an instance of a text editor and USB analyzer software on each computer. Step 2: Connect the first computer to the TOE and ensure it is selected and that no other computers are connected. Step 3: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer. Step 4: Disconnect the first computer. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. Step 5: Cease generation of the USB HID traffic, connect the second computer to the same port and ensure it is selected. Step 6: Verify that no results from the previous use of the peripheral device are observed on the selected computer and that no traffic is sent and captured using the USB analyzer. Step 7: Reboot the TOE and repeat step 6. Step 8: Turn off the TOE and repeat step 6. Step 9: Restart the TOE and repeat step 6. Step 10: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, USBlyzer, Dell P2319H Monitor.
Test Execution Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Connect two computers to a different display and run an instance of a text editor and USB analyzer software on each computer. 2. Connect the first computer to the TOE and ensure it is selected and that no other computers are connected. 3. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer. 4. Disconnect the first computer. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. 5. Cease generation of the USB HID traffic, connect the second computer to the same port and ensure it is selected. 6. Verify that no results from the previous use of the peripheral device are observed on the selected computer and that no traffic is sent and captured using the USB analyzer. 7. Reboot the TOE and repeat step 6. 8. Turn off the TOE and repeat step 6. 9. Restart the TOE and repeat step 6.

	10. Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.		
Execution Output	1. The evaluator ensured authorized peripheral devices were connected, a display was connected to each computer and a text editor and USB analyzer application was running on each computer. 2. The evaluator ensured only the first computer was connected and selected, no other computers were connected. 3. The evaluator exercised the functions of the peripheral device types and verified that the USB traffic was captured on selected computer. 4. The evaluator ensured the first computer was disconnected. The evaluator generated intense HID traffic using the keyboard and mouse. 5. HID USB traffic generation was ceased. The evaluator connected the second computer to the same port and ensured it was selected. 6. The evaluator confirms that no USB traffic leaked over from the first computer. 7. The evaluator rebooted the TOE. No USB data was captured. 8. The evaluator powered off the TOE. No USB data was captured. 9. The evaluator restarted the TOE. No USB data was captured. The evaluator exercised the functions of the peripheral device types and verified that the expected USB traffic was generated on selected computer.		
Pass/Fail Explanation	Data flow through the same interface has been observed and tested. The evaluator confirmed that the TOE does not send data to different computers connected to the same interface at different times. No residual USB traffic from other computers connected to the same port was observed during power cycles. USB traffic was seen only on the connected and selected computer.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.13 FDP_APC_EXT.1/UA Test 1

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/UA – Test 1*
Objective	For tests that use the USB sniffer or USB analyzer software, the evaluator verifies whether traffic is sent or not sent by inspection of the passing USB transactions and ensuring they do not contain USB data payloads other than any expected traffic, as well as USB NAK transactions or system messages. To avoid clutter during USB traffic capture, the evaluator may filter NAK transactions and system messages. Test Setup For each of the below tests the evaluator shall perform the following test set up: 1. Configure the TOE and the operational environment in accordance with the operational guidance. 2. Connect a computer to each TOE UA computer interface and a display to each connected computer. 3. Open a real-time hardware information console and USB protocol analyzer software on each connected computer.

	4. Ensure the user authentication application and driver for the authorized user authentication device used for testing is installed. 5. [Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:] connect an authorized user authentication device with a power LED and a connected DVM to each PSD UA peripheral device interface. Test 1-UA: UA Switching methods [Conditional: Perform this test if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP] This test verifies the functionality of the TOE’s UA switching methods. While performing this test, ensure that switching is always initiated through express user action. Step 1. Turn on the TOE and ensure computer #1 is selected. Step 2: Verify that the real-time hardware information console on computer #1 indicates the presence of the user authentication device. [Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:] verify the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC. Step 3: Perform steps 4-6 for each connected computer. Step 4: For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational guidance. Step 5: [Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:] verify that the LED for the UA device is not illuminated for at least one second while the DVM reads 0.5 VDC or less for at least one second. Step 6: Verify that the real-time hardware console on the newly selected computer indicates the presence of the user authentication device. [Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:] verify the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Device Manager, Keweisi USB Detector, Identiv USB UA Device, Fluke True RMS Digital Multimeter, Dell P2319H Monitor.
Test Execution Steps	1. Turn on the TOE and ensure computer #1 is selected. 2. Verify that the real-time hardware information console on computer #1 indicates the presence of the user authentication device. *[Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:]* verify the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC. 3. Perform steps 4 - 6 for each connected computer. 4. For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational guidance. 5. *[Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:]* verify that the LED for the UA device is not illuminated for at least one second while the DVM reads 0.5 VDC or less for at least one second. 6. Verify that the real-time hardware console on the newly selected computer indicates the presence of the user authentication device. *[Conditional: if “external” is selected in FDP_PDC_EXT.4.1, then:]* verify the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC.
Execution Output	1. The evaluator ensured the TOE was powered on and computer #1 was selected.

	2. The evaluator verifies that the hardware information console indicates a user authentication device. The evaluator verifies that the UA device power LED is illuminated and the DVM reads between 4.75 and 5.25 VDC. 3. The evaluator repeated steps 4 – 6 for each computer. 4. The evaluator switched selected computers for each switching method selected in FDP_SWI_EXT.2.2. 5. The evaluator verified that the LED for the UA device was not illuminated for at least one second while the DVM reads 0.5 VDC or less for at least one second. 6. The evaluator verified the presence of the user authentication device in a real-time hardware console. The DVM read between 4.74 and 5.25 VDC.		
Pass/Fail Explanation	The evaluator confirmed that the functionality of the TOE's UA switching methods is successful. The hardware console indicates a UA device, the power LED was in the correct state and the correct voltages were observed for each condition.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.14 FDP_APC_EXT.1/UA Test 2

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/UA – Test 2*
Objective	Test 2-UA: Positive and Negative UA Data Flow Rules Testing This test verifies correct data flows of a UA device during different power states of the selected computer. Step 1: For each connected computer, connect a USB sniffer between it and the TOE or ensure the USB analyzer software is opened. Perform steps 2-14 with each connected computer as the selected computer. Step 2: Connect an authentication session and verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer. Step 3: Remove the authentication element and verify the session is terminated on the selected computer. Step 4: Insert the authentication element. Reconnect an authentication session, verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer [Conditional: Perform steps 5-6 if "external" is selected in FDP_PDC_EXT.4.1.] Step 5: Disconnect the UA device and verify the session is terminated on the selected computer and that the real-time hardware console does not show the device and that no traffic is sent on the USB analyzer. Step 6: Reconnect the UA device. Reconnect an authentication session, verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer. [Conditional: Perform steps 7-14 if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.]

	Step 7: Verify that the real-time hardware console on each of the non-selected computers does not show the UA device and that no traffic is sent on the other USB analyzers. Step 8: Switch to another connected computer. Verify that the authentication session on the previously selected computer is terminated, the real-time hardware console on each non-selected computer does not show the UA device, and that no traffic is sent on the other USB analyzers. Step 9: Connect an authentication session and verify that the session is connected on the selected computer, the expected traffic is sent and captured using the USB analyzer, and no traffic is sent on the other USB analyzers. Step 10: Switch to the originally selected computer. Verify the authentication session is still terminated, and reconnect an authentication session. Verify that no traffic is sent on the other USB analyzers. Step 11: Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent. Step 12: Reconnect an authentication session and verify that no traffic is sent on the other USB analyzers. Reboot the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent. Step 13: Reconnect an authentication session and verify that no traffic is sent on the other USB analyzers. Enter sleep or suspend mode in the selected computer. Examine the USB analyzers on each of the nonselected computers and verify that no traffic is sent. Step 14: Exit sleep or suspend mode in the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent. Step 15: Perform steps 16-17 when the TOE is off and then in a failure state. Step 16: Verify that for each connected computer, no real-time hardware console shows the device and no traffic is sent on the USB analyzer. Step 17: Verify the authentication session is terminated on the selected computer.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, USBlyzer, Identiv USB UA Device, Device Manager, Dell P2319H Monitor.
Test Execution Steps	1. For each connected computer, connect a USB sniffer between it and the TOE or ensure the USB analyzer software is opened. Perform steps 2-14 with each connected computer as the selected computer. 2. Connect an authentication session and verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer. 3. Remove the authentication element and verify the session is terminated on the selected computer. 4. Insert the authentication element. Reconnect an authentication session, verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

	5. *[Conditional: Perform steps 5-6 if "external" is selected in FDP_PDC_EXT.4.1.]* Disconnect the UA device and verify the session is terminated on the selected computer and that the real-time hardware console does not show the device and that no traffic is sent on the USB analyzer. 6. Reconnect the UA device. Reconnect an authentication session, verify that the session is connected on the selected computer and that the expected traffic is sent and captured using the USB analyzer. 7. [Conditional: Perform steps 7-14 if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.] Verify that the real-time hardware console on each of the non-selected computers does not show the UA device and that no traffic is sent on the other USB analyzers. 8. Switch to another connected computer. Verify that the authentication session on the previously selected computer is terminated, the real-time hardware console on each non-selected computer does not show the UA device, and that no traffic is sent on the other USB analyzers. 9. Connect an authentication session and verify that the session is connected on the selected computer, the expected traffic is sent and captured using the USB analyzer, and no traffic is sent on the other USB analyzers. 10. Switch to the originally selected computer. Verify the authentication session is still terminated and reconnect an authentication session. Verify that no traffic is sent on the other USB analyzers. 11. Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent. 12. Reconnect an authentication session and verify that no traffic is sent on the other USB analyzers. Reboot the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent. 13. Reconnect an authentication session and verify that no traffic is sent on the other USB analyzers. Enter sleep or suspend mode in the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent. 14. Exit sleep or suspend mode in the selected computer. Examine the USB analyzers on each of the non-selected computers and verify that no traffic is sent. 15. Perform steps 16-17 when the TOE is off and then in a failure state. 16. Verify that for each connected computer, no real-time hardware console shows the device and no traffic is sent on the USB analyzer. 17. Verify the authentication session is terminated on the selected computer.
Expected Output	1. USB sniffer setup correctly and USB analyzer software is open on the computer. 2. USB analyzer traffic is generated, and authentication session is active. 3. Authentication session is terminated. 4. USB analyzer traffic is generated, and authentication session is active. 5. Authentication session is terminated, and no USB traffic is captured. 6. USB analyzer traffic is generated, and authentication session is active. 7. Non-selected computers do not show UA device and no USB traffic is generated. 8. Authentication session will be terminated, hardware console does not recognize UA device, and no USB traffic is generated.

	9. Authentication session is active and expected USB traffic is generated only on selected computer. 10. No USB traffic is generated on other USB analyzers. 11. No USB traffic is generated on non-selected computers. 12. No USB traffic is generated on non-selected computers. 13. No USB traffic is generated on non-selected computers. 14. No USB traffic is generated on non-selected computers. 15. Steps repeated while TOE is OFF and then in failure state. 16. Hardware console does not show device, no USB traffic is generated on non-selected computers. 17. Authentication session will be closed.		
Pass/Fail Explanation	The evaluator confirmed correct data flows of a UA device during different power states of the selected computer. No USB traffic was observed on non-selected computers.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.15 FDP_APC_EXT.1/UA Test 3

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/UA – Test 3*
Objective	Test 3-UA: No Electrical Flow between Computer Interfaces. [Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP] This test verifies no electrical signals flow between connected computers when the TOE is powered on or off. Perform this test for each TOE UA computer interface. Perform this test when the TOE is powered on and off. Step 1: Disconnect the first computer and replace it with a switchable 5 volt power supply with a USB Type-B plug. Modulate the 5 volt supply manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on the non-selected USB analyzers. [Conditional: Perform steps 2-4 if "external" is selected in FDP_PDC_EXT.4.1.] Step 2: Disconnect the power supply and replace it with the computer. Step 3: Connect the USB dummy load into the TOE UA peripheral device interface. Examine the USB analyzers on all non-selected computers and verify that no new USB traffic is captured. Step 4: Disconnect the USB dummy load and replace it with a switchable 5 volt power supply with a USB Type-B plug. Modulate the 5 volt supply manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on the non-selected USB analyzers.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dr. Meter DC Power Supply, HSL USB Dummy Load, USBlyzer, Dell P2319H Monitor, Spliced USB Type-B Cable.

Test Execution Steps	1. [Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP] This test verifies no electrical signals flow between connected computers when the TOE is powered on or off. Perform this test for each TOE UA computer interface. Perform this test when the TOE is powered on and off. Disconnect the first computer and replace it with a switchable 5-volt power supply with a USB Type-B plug. Modulate the 5-volt supply manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on the non-selected USB analyzers. 2. *[Conditional: Perform steps 2-4 if "external" is selected in FDP_PDC_EXT.4.1.]* Disconnect the power supply and replace it with the computer. 3. Connect the USB dummy load into the TOE UA peripheral device interface. Examine the USB analyzers on all non-selected computers and verify that no new USB traffic is captured. 4. Disconnect the USB dummy load and replace it with a switchable 5-volt power supply with a USB Type-B plug. Modulate the 5 volts supply manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on the non-selected USB analyzers.		
Execution Output	1. The evaluator disconnected the first computer and replaced it with a switchable 5-volt power supply with a USB type-B plug. The evaluator modulated the 5-volt supply at various speeds and confirmed that no USB traffic was generated on non-selected computers. 2. The evaluator disconnected the power supply and replaced it with the computer. 3. The evaluator connected a USB dummy load into the TOE UA peripheral device interface. The evaluator confirms that no USB traffic was generated on non-selected computers. 4. The evaluator disconnected the USB dummy load and replaced it with a switchable 5-volt power supply with a USB type B plug. The evaluator modulated the 5-volt supply at various speeds and confirmed that no USB traffic was generated on non-selected computers.		
Pass/Fail Explanation	The evaluator confirmed that no electric signals or USB traffic flow between connected computers when the TOE is powered on or off.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.16 FDP_APC_EXT.1/UA Test 4

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/UA – Test 4*
Objective	Test 4-UA: No Flow between Connected Computers over Time This test verifies that the TOE does not send data to different computers connected to the same interface at different times. Repeat this test for each TOE UA computer port. Note that instead of the session ID, the evaluator may substitute authentication element or other unique session identification characteristic detectable by the USB analyzer. Step 1: Ensure only one computer is connected to the TOE and it is selected.

	Step 2: Connect an authentication session and record the authentication session ID using the USB analyzer. Step 3: Disconnect the first computer, connect the second computer to the same port, connect an authentication session, and record the authentication session ID in less time than the authentication device timeout. Step 4: Verify that the authentication session ID is different. Step 5: Disconnect the second computer, connect the first computer to the same port, reconnect the authentication session, and record the authentication session ID in less time than the authentication device timeout. Step 6: Verify that the authentication session ID is different from the first two.		
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, USBlyzer, Identiv USB UA Device, Dell P2319H Monitor.		
Test Execution Steps	1. Ensure only one computer is connected to the TOE and it is selected. 2. Connect an authentication session and record the authentication session ID using the USB analyzer. 3. Disconnect the first computer, connect the second computer to the same port, connect an authentication session, and record the authentication session ID in less time than the authentication device timeout. 4. Verify that the authentication session ID is different. 5. Disconnect the second computer, connect the first computer to the same port, reconnect the authentication session, and record the authentication session ID in less time than the authentication device timeout. 6. Verify that the authentication session ID is different from the first two.		
Execution Output	1. The evaluator ensured that only one computer was connected to the TOE and it was selected. 2. The evaluator connected an authentication sessions and recorded the session ID using the USB analyzer. 3. The evaluator disconnected the first computer and connected the second computer to the same port. An authentication session was open with the Session ID being recorded. 4. The evaluator verified that the sessions ID was different from Step 2's session ID. 5. The evaluator disconnected the second computer and connected the first computer to the same port. An authentication session was open with the session ID being recorded. 6. The evaluator verified that the sessions ID was different from Step 2 and 4 sessions ID.		
Pass/Fail Explanation	The evaluator confirms that the TOE does not send data to different computers connected to the same interface at different times. All session IDs were associated with the correct computer.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.17 FDP_APC_EXT.1/VI Test 1

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/VI – Test 1*

Objective	Test 1-VI: Video Source Selection and Identification, TOE Off and Failure States This test verifies the TOE switching function operates properly and will stop the video output display when in an OFF or FAILURE state. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Step 2: Play a different video with embedded audio on a number of computers for each TOE computer video interface. Step 3: Connect each computer to a TOE computer video interface. Step 4: Connect a display to each TOE display interface. Step 5: Turn on the TOE. Step 6: For each connected computer, ensure it is selected and verify that the video and its accompanying audio from the selected computer(s) are received on the proper display(s). Step 7: [Conditional: if the TOE claims the Combiner Use Case then] verify that video generated by the TOE has clear identification marking or text to properly identify the source computer shown. Step 8: Turn off the TOE and verify that no video appears on any connected display. Step 9: Power on the TOE and cause the TOE to enter a failure state. Verify that the TOE provides the user with a visual indication of failure and that no usable video appears on any connected display. Step 10: Repeat steps 3 to 9 for each unique display protocol and port type supported by the TOE.
Notes	• TD0539 applied.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Edifier Multimedia Speaker, Dell P2319H Monitor.
Test Execution Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. 2. Play a different video with embedded audio on a number of computers for each TOE computer video interface. 3. Connect each computer to a TOE computer video interface. 4. Connect a display to each TOE display interface. 5. Turn on the TOE. 6. For each connected computer, ensure it is selected and verify that the video and its accompanying audio from the selected computer(s) are received on the proper display(s). 7. *[Conditional: if the TOE claims the Combiner Use Case then]* verify that video generated by the TOE has clear identification marking or text to properly identify the source computer shown. 8. Turn off the TOE and verify that no video appears on any connected display. 9. Power on the TOE and cause the TOE to enter a failure state. Verify that the TOE provides the user with a visual indication of failure and that no usable video appears on any connected display. 10. Repeat steps 3 to 9 for each unique display protocol and port type supported by the TOE.
Execution Output	1. The evaluator ensured the TOE was configured correctly.

	2. The evaluator played different videos with embedded audio on a number of computers for each TOE computer video interface. 3. The evaluator connected each computer to a TOE computer video interface. 4. The evaluator ensured a display was connected to each TOE display interface. 5. The TOE was powered on. 6. For each connected computer the evaluated ensured it was selected. The evaluator verified that the video and its accompanying audio are received on the proper displays. 7. The evaluator ensured the video and accompanying audio from the selected computers contain identifications markings which properly identify the source computer shown. 8. The evaluator turned off the TOE and verified that no video appeared on any connected display. 9. The evaluator caused the TOE to enter a failure state and ensured the visual indication of a failure state was present (TOE cycles between LED front panel indicator channels). No usable video appeared on any connected display. 11. The evaluator repeated steps 3 – 9 for each unique display protocol and port type supported by the TOE.		
Pass/Fail Explanation	The evaluator confirmed that the TOE switching function operates properly and only on the selected computer, and will stop the video output display when in an OFF or FAILURE state.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.18 FDP_APC_EXT.1/VI Test 2

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/VI – Test 2*
Objective	Test 2-VI: Computer Video Interface Isolation [Conditional: perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP.] This test verifies that the TOE does not transfer data to any non-selected computer video interface. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect only the first computer interface cable to one computer. Turn on the TOE. Step 2: Switch the TOE primary display to computer #1. Step 3: Observe the primary display to verify that the selected computer is the one that is shown. Step 4: Remove the non-selected computer video interface cables from the TOE and connect the oscilloscope probe to the TOE #2 computer video interface to verify that no SYNC signal is passed through the TOE. Based on the connection interface protocol, this is performed as follows: 1. Video Graphics Array (VGA) – single ended probe on pins 13 and then 14;

	2. High-Definition Multimedia Interface (HDMI) – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide Hot Plug Detect (HPD) signal; Check for signals - differential probe between pins 10 (+) and 12 (-); 3. Digital Visual Interface (DVI)-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-); 4. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-); 5. DisplayPort - connect pin 18 to a 3.3V power supply via 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+); 6. USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11. Step 5: Repeat steps 3 and 4 while selecting other TOE connected computers. Verify that no SYNC signal is present. Step 6: Repeat steps 3 to 5 with the TOE unpowered. Verify that no SYNC signal is present. Step 7: With the probe connected to the TOE computer #2 video interface, disconnect / reconnect the computer #1 video cable. Power up the TOE and select computer #1. Attempt to detect the change in the oscilloscope at each one of the TOE #2 computer video interface pins. No changes shall be detected. Step 8: Repeat step 7 for each one of the other TOE computer video interfaces. Step 9: Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, disconnect and reconnect the display. Step 10: Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, reboot the selected computer. Step 11: Repeat steps 2 to 10 with each connected computer. Step 12: [Conditional: if “multiple connected displays” is selected in FDP_CDS_EXT.1.1 then] repeat steps 3 to 10 with each other display connected to the TOE. Step 13: Repeat this test for each unique display protocol and port type supported by the TOE.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Tektronix Oscilloscope, Dr. Meter DC Power Supply, Dell P2319H Monitor, Spliced HDMI Cable, Spliced DisplayPort Cable, Spliced USB Type-C Cable.
Test Execution Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect only the first computer interface cable to one computer. Turn on the TOE. 2. Switch the TOE primary display to computer #1. 3. Observe the primary display to verify that the selected computer is the one that is shown.

	4. Remove the non-selected computer video interface cables from the TOE and connect the oscilloscope probe to the TOE #2 computer video interface to verify that no SYNC signal is passed through the TOE. Based on the connection interface protocol, this is performed as follows: 1**. Video Graphics Array (VGA)** – single ended probe on pins 13 and 14; 2. **High-Definition Multimedia Interface (HDMI)** – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide Hot Plug Detect (HPD) signal; Check for signals - differential probe between pins 10 (+) and 12 (-); 3**. Digital Visual Interface (DVI)-I** – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-); 4. **DVI-D** - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-); 5. **DisplayPort** - connect pin 18 to a 3.3V power supply via 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+); 6. **USB Type-C with DisplayPort as Alternate Function** – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11 5. Repeat steps 3 and 4 while selecting other TOE connected computers. Verify that no SYNC signal is present. 6. Repeat steps 3 to 5 with the TOE unpowered. Verify that no SYNC signal is present. 7. With the probe connected to the TOE computer #2 video interface, disconnect / reconnect the computer #1 video cable. Power up the TOE and select computer #1. Attempt to detect the change in the oscilloscope at each one of the TOE #2 computer video interface pins. No changes shall be detected. 8. Repeat step 7 for each one of the other TOE computer video interfaces. 9. Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, disconnect and reconnect the display. 10. Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, reboot the selected computer. 11. Repeat steps 2 to 10 with each connected computer. 12. [*Conditional: if "multiple connected displays" is selected in FDP_CDS_EXT.1.1 then]* repeat steps 3 to 10 with each other display connected to the TOE. 13. Repeat this test for each unique display protocol and port type supported by the TOE.
Execution Output	1. The evaluator ensured the TOE was configured correctly. The evaluator connected only the first computer interface cable to one computer. The evaluator ensured the TOE was powered on. 2. The evaluator ensured the TOE primary display was on computer #1. 3. The evaluator confirmed that the selected computer is the one that is shown. 4. The evaluator removed the non-selected computer video interface cables from the TOE and connected the oscilloscope probe to the TOE #2 computer video interface. The evaluator verified that no SYNC signal was passed through the TOE based on the corresponding connection interface protocol. 5. The evaluator repeated steps 3 and 4 while selecting other TOE connected computers. The evaluator confirmed that no SYNC signal was present.

	6. The evaluator repeated steps 3 to 5 with the TOE unpowered. The evaluator confirmed no SYNC signal was present. 7. The evaluator connected the probe to TOE computer #2 video interface and disconnected / reconnected the computer #1 video cable. The evaluator powered up the TOE and selected computer #1. The evaluator attempted to detect the change in the oscilloscope at each of the TOE #2 computer video interface pins, but no change in oscilloscope was detected. 8. The evaluator repeated step 7 for each one of the other TOE computer video interfaces. No change was detected in any other interface. 9. The evaluator repeated steps 7 and 8, but instead of disconnected / reconnected the computer the evaluator disconnected and reconnected the display. No change was detected in any of the interfaces when disconnecting and reconnecting the display. 10. The evaluator repeated steps 7 and 8, but instead of disconnecting / reconnecting the computer, the evaluator reboot the selected computer. No change was detected in any of the interfaces when rebooting the selected computer. 11. The evaluator repeated steps 2 to 10 wth each connected computer. All tests passed for each connected computer. 12. The evaluator repeated steps 3 to 10 with each other displaye connected to the TOE. All tests passed for secondary display. 13. The evaluator repeated this test for each unique display protocol.		
Pass/Fail Explanation	The evaluator confirms that the TOE does not transfer data to any non-selected computer video interface. No SYNC signal was received on non-selected computers.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.19 FDP_APC_EXT.1/VI Test 3

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/VI – Test 3*
Objective	3-VI - Unauthorized Sub-protocols Note that in the following steps only native video protocol cables shall be used. No conversion from other video protocols is allowed in these tests except as directed in FDP_IPC_EXT.1.1. This test verifies that unauthorized sub-protocols are blocked. TD0514 has been applied. Perform this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.1. In the following steps the evaluator shall establish a verified test setup that passes video signals across the TOE. Step 1: Connect at least one computer with a native video protocol output to the TOE computer #1 video input interface. Step 2: Connect at least one display with native video protocol to the TOE display output. Step 3: Power up the TOE and ensure the connected computer is selected.

	Step 4: Verify that the video image is visible and stable on the user display. In the following steps the evaluator shall verify that the test setup properly blocks the unauthorized video sub-protocol traffic. Step 5: Open the Monitor Control Command Set (MCCS) control console program on the computer and attempt to change the display contrast and brightness. Verify that the display does not change its contrast and brightness accordingly. Step 6: Disconnect the video cable connecting the display and the TOE and connect the display directly to the computer. Verify that the video image is visible and stable on the user display. Step 7: Attempt to change the display contrast and brightness. Verify that the display does change its contrast and brightness accordingly. Step 8: Connect the following testing device based on the display video protocol being tested at the peripheral display interface: 1. DisplayPort – DisplayPort AUX channel analyzer in series between the display and the TOE 2. HDMI – HDMI sink test device 3. USB Type-C with DisplayPort as Alternate Function – USB sniffer in series between the display and the TOE 4. VGA – VGA sink test device 5. DVI-I/DVI-D – DVI sink test device Step 9: Attempt to change the display contrast and brightness. Verify that the testing device does not capture any MCCS commands. Step 10: Replace the computer with a source generator for each selected protocol at the computer video interface. If DVI-I or DVI-D is selected, use an HDMI source generator. Step 11: Run an EDID write transaction at the generator and verify in the testing device that no EDID traffic is captured. Step 12: [Conditional, if DisplayPort, DVI-D, DVI-I, HDMI, or USB Type-C is the selected protocol being tested at the computer video interface, then] run Consumer Electronics Control (CEC) and High-bandwidth Digital Content Protection (HDCP) tests or commands at the generator and verify in the testing device that no CEC or HDCP traffic is captured. Step 13: [Conditional, if DVI-D, DVI-I, or HDMI is the selected protocol being tested at the computer video interface, then] run Audio Return Channel (ARC), HDMI Ethernet and Audio Return Channel (HEAC), and HDMI Ethernet Channel (HEC) tests or commands at the generator and verify in the testing device that no ARC, HEAC, or HEC traffic is captured. Step 14: [Conditional: If “[HDMI] protocol” is selected in FDP_IPC_EXT.1.2, then] perform steps 15 and 16 for both pin 13 (CEC) and 14 (UTILITY). Step 15: Turn off the TOE. Use a multi-meter to measure the resistance-to-ground of the pin at the TOE HDMI peripheral interface and verify it is greater than 2 Mega-ohms.

	Step 16: Attach a single ended oscilloscope probe between the pin and the ground, turn on the TOE, and verify that no changes between 0.0v and 0.2v and between 3.0v and 3.3v are detected. Step 17: [Conditional: if VGA is not the selected protocol being tested, then] disconnect all devices. Connect the display to a TOE computer video interface and the oscilloscope to the TOE display interface in order to verify that no HPD signal is passed by measuring a signal voltage of less than 1.0V. Based on the selected protocol being tested, this is performed as follows: 1. HDMI – connect scope to pin 19 and verify no HPD signal is detected; 2. DVI-D/DVI-I – connect scope to pin 16 and verify no HPD signal is detected; 3. DisplayPort - connect scope to pin 18 and verify no HPD signal is detected; 4. USB Type-C with DisplayPort as Alternate Function – connect scope to pin A8 and B8 and verify no HPD signal is detected. Step 18: Repeat this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.2.
Notes	• TD0514 applied. • TD0584 applied.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, SoftMCCS, DisplayPort Aux Channel Monitor, Unigraf DPA-400 DisplayPort Aux Channel Monitor, QuantumData 882E Video Test Generator, Fluke True RMS Digital Multimeter, Tektronix Oscilloscope, QuantumData 980 Video Test Generator, TCL 40” Smart TV with ARC, Spliced HDMI Cable, Spliced DisplayPort Cable, Spliced USB Type-C Cable, Dell P2319H Monitor.
Test Execution Steps	1. Connect at least one computer with a native video protocol output to the TOE computer #1 video input interface. 2. Connect at least one display with native video protocol to the TOE display output. 3. Power up the TOE and ensure the connected computer is selected. 4. Power up the TOE and ensure the connected computer is selected. 5. Open the Monitor Control Command Set (MCCS) control console program on the computer and attempt to change the display contrast and brightness. Verify that the display does not change its contrast and brightness accordingly. 6. Disconnect the video cable connecting the display and the TOE and connect the display directly to the computer. Verify that the video image is visible and stable on the user display. 7. Attempt to change the display contrast and brightness. Verify that the display does change its contrast and brightness accordingly. 8. Connect the following testing device based on the display video protocol being tested at the peripheral display interface: 1. DisplayPort – DisplayPort AUX channel analyzer in series between the display and the TOE 2. HDMI/DVI-I/-DVI-D – HDMI sink test device 3. USB Type-C with DisplayPort as Alternate Function – USB sniffer in series between the display and the TOE 4. VGA – VGA sink test device

	9. Attempt to change the display contrast and brightness. Verify that the testing device does not capture any MCCS commands. 10. Replace the computer with a source generator for each selected protocol at the computer video interface. If DVI-I or DVI-D is selected, use an HDMI source generator. 11. Run an EDID write transaction at the generator and verify in the testing device that no EDID traffic is captured. 12. *[Conditional, if DisplayPort, DVI-D, DVI-I, HDMI, or USB Type-C is the selected protocol being tested at the computer video interface, then]* run Consumer Electronics Control (CEC) and High-bandwidth Digital Content Protection (HDCP) tests or commands at the generator and verify in the testing device that no CEC or HDCP traffic is captured. 13. *[Conditional, if DVI-D, DVI-I, or HDMI is the selected protocol being tested at the computer video interface, then]* run Audio Return Channel (ARC), HDMI Ethernet and Audio Return Channel (HEAC), and HDMI Ethernet Channel (HEC) tests or commands at the generator and verify in the testing device that no ARC, HEAC, or HEC traffic is captured. 14. *[Conditional: If "[HDMI] protocol" is selected in FDP_IPC_EXT.1.2, then]* perform steps 15 and 16 for both pin 13 (CEC) and 14 (UTILITY). 15. Turn off the TOE. Use a multi-meter to measure the resistance-to-ground of the pin at the TOE HDMI peripheral interface and verify it is greater than 2 Mega-ohms. 16. Attach a single ended oscilloscope probe between the pin and the ground, turn on the TOE, and verify that no changes between 0.0v and 0.2v and between 3.0v and 3.3v are detected. 17. *[Conditional: if VGA is not the selected protocol being tested, then]* disconnect all devices. Connect the display to a TOE computer video interface and the oscilloscope to the TOE display interface in order to verify that no HPD signal is passed by measuring a signal voltage of less than 1.0V. Based on the selected protocol being tested, this is performed as follows: 1. HDMI – connect scope to pin 19 and verify no HPD signal is detected; 2. DVI-D/DVI-I – connect scope to pin 16 and verify no HPD signal is detected; 3. DisplayPort - connect scope to pin 18 and verify no HPD signal is detected; 4. USB Type-C with DisplayPort as Alternate Function – connect scope to pin A8 and B8 and verify no HPD signal is detected. 18. Repeat this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.2
Execution Output	1. The evaluator ensured at least one computer with native video protocol output was connected to the TOE computer #1 video input interface. 2. The evaluator ensured at least one display with native video protocol was connected to TOE display output. 3. The evaluator ensured the TOE was powered up. The connected video was selected. 4. The evaluator confirmed that the image was visible and stable on the user display. 5. The evaluator opened the monitor control command set control console program on the computer and attempted to change the display contrast and brightness. The evaluator confirms the display contrast and brightness did not change.

	6. The evaluator disconnected the video cable connecting the display and the TOE and connected the display directly to the computer. The video image was visible and stable on the user display. 7. The evaluator attempted to change the display contrast and brightness. The contrast and brightness did change accordingly. 8. The evaluator connected the testing device based on display video protocol. 9. The evaluator attempted to change the display contrast and brightness. The evaluator confirms no MCCS commands were captured. 10. The evaluator replaced the computer with a source generator for each selected protocol at the computer video interface. 11. The evaluator ran an EDID write transation at the generator and verified that no EDID traffic was captured. 12. The evaluator ran CEC and HDCP tests at the generator and confirmed that no CEC or HDCP traffic was captured. 13. The evaluator ran the ARC, HEAC and HEC tests at the generator and confirmed no ARC, HEAC or HEC traffic was captured. 14. The evaluator performed steps 15 and 16 for both pins 13 (CEC) and 14 (UTILITY). 15. The evaluator turned off the TOE. The evaluator confirmed that the multi-meter reads greater than 2 Mega-ohms. 16. The evaluator confirmed no changes between 0.0v and 0.2v and between 3.0 and 3.3v were detected on the oscilloscope. 17. The evaluator confirmed no HPD signal was passed by measuring a signal voltage of less than 1.0 v. 18. The evaluator ensured to repeat this tests for of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.2.		
Pass/Fail Explanation	The evaluator has confirmed that the TOE successfully blocks unauthorized sub-protocols. No EDID, MCCS, CEC, or HDCP traffic was observed. All readouts from the testing tools were in the proper voltage ranges when expected.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.20 FDP_APC_EXT.1/VI Test 4

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/VI – Test 4*
Objective	Test 4-VI - Video and EDID Channel Unidirectional Rule This test verifies that the TOE video path is unidirectional from the computer video interface to the display interface with the exception of EDID, which may be read from the display once at power up and then may be read by the connected computers. The evaluator should have at least two high-resolution displays of different models and one low-resolution displays o for each TOE-supported video protocol. In the following steps the evaluator should attempt to read display EDID after the TOE completed its self-test / power up. The TOE should not read the new display EDID. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance.

	Connect a computer and a high-resolution display to the TOE. Step 2: Ensure the TOE is on, computer #1 is selected, and verify that the display shows video from computer #1 as expected. Step 3: Turn off the TOE. Disconnect the user display from the TOE. Step 4: Connect the low-resolution display to the TOE and turn on the TOE. After the video is shown on the display, turn off the TOE and disconnect the low-resolution display. Step 5: Turn on the TOE. After the TOE has completed the self-test, the TOE may fail to generate video on the user display (i.e., no EDID is read at the TOE power up). If the display is showing video, then run the EDID reading and parsing software on computer #1 and check that there is no active EDID (i.e., the computer is using a default generic display or reading older display settings from the registry). In the following steps the evaluator shall validate that the TOE video path is unidirectional from the computer video interface to the display interface. Step 6: Perform steps 7-11 for each TOE computer video interface. Step 7: Power off the TOE and disconnect the computer #1 video output and the display. Connect the display cable to the TOE computer #1 video interface. Connect the computer #1 video cable to the TOE display interface. This configuration will attempt to force video data through the TOE in the reverse direction. Step 8: Power up the TOE again. Step 9: Check that the video is not visible in the display. Step 10: Perform steps 11 while the TOE is powered on and powered off. Step 11: Remove the display cable from the TOE and connect the oscilloscope to verify that no SYNC signal is passed through the TOE. Based on the video protocols supported, this is performed as follows: 1. VGA – single ended probe on pins 13 and 14; 2. HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - differential probe between pins 10 (+) and 12 (-); 3. DVI-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-); 4. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-); 5. DisplayPort - connect pin 18 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+); 6. USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11.
Notes	• TD0506 applied.

Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor, Asus PA238 Monitor, Dell 1907FPc Monitor, Tektronix Oscilloscope, Dr. Meter DC Power Supply, Spliced HDMI Cable, Spliced DisplayPort Cable, Spliced USB Type-C Cable.		
Execution Output	1. The evaluator ensured the TOE was configured correctly. The evaluator ensured a computer and high-resolution display were connected to the TOE. 2. The evaluator ensured the TOE was on and that computer #1 was selected. The evaluator verified that the display shows video from computer #1. 3. The evaluator ensured the TOE was powered off. The display was disconnected from the TOE. 4. The evaluator connected a low-resolution display to the TOE and turned on the TOE. The video was successfully shown on the display, and then the TOE was turned off and the low-resolution display was disconnected. 5. The evaluator turned on the TOE. The display shows video correctly and the evaluator ran the EDID reading and parsing software on computer #1. The evaluator confirms there is no active EDID. 6. The evaluator ensured steps 7 - 11 were performed for each TOE computer video interface. 7. The evaluator connected computer #1 video output to the TOE display port, and display cable to the computer #1 video interface. 8. The TOE was powered up again. 9. The evaluator confirms that no video was visible in the display. 10. The evaluator performed steps 11 while the TOE was powered off and powered on. 1. The evaluator emoved the display cable from the TOE and connected an oscilloscope. The evaluator verified that no SYNC signal was passed through the TOE.		
Pass/Fail Explanation	The evaluator confirms the TOE video path is unidirectional from the computer video interface to the display interface except for EDID.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.21 FDP_APC_EXT.1/VI Test 5

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/VI – Test 5*
Objective	Test 5-VI – No Flow between Connected Computers over Time This test verifies that the TOE does not send data to different computers connected to the same TOE video interface over time. Repeat this test for each TOE Video port. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Run EDID reading and parsing software on two computers and connect a display to the TOE. Step 2: Connect computer #1 to the TOE, ensure the TOE is on, computer #1 is selected, no other computers are connected, and verify that the display shows video from computer #1 as expected.

	Step 3: Capture the TOE EDID content in the software on computer #1 and save as a file with a name that indicates capture time. Step 4: Disconnect computer #1 and connect an I2C programmer to the same port. Attempt to write the characters “FFFF” over the entire EDID address range. Step 5: Disconnect the I2C programmer, reconnect computer #1 to the same port, and repeat step 3. Step 6: Reboot the TOE and repeat step 3. Step 7: Turn off the TOE and repeat step 3. Step 8. Restart the TOE and repeat step 3. Step 9: Disconnect computer #1 and repeat steps 2 to 8 with computer #2 on the same port. Step 10: Repeat steps 2 to 9 for a total of 20 EDID file captures. Step 11: Collect all 20 captured EDID files, compare them bit-by-bit, and verify that they are identical excluding null captures recorded in Step 7..
Notes	• TD0584 applied.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Monitor Asset Manager, QuantumData 980 Video Test Generator, QuantumData 882E Video Test Generator, Dell P2319H Monitor.
Test Execution Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Run EDID reading and parsing software on two computers and connect a display to the TOE. 2. Connect computer #1 to the TOE, ensure the TOE is on, computer #1 is selected, no other computers are connected, and verify that the display shows video from computer #1 as expected. 3. Capture the TOE EDID content in the software on computer #1 and save as a file with a name that indicates capture time. 4. Disconnect computer #1 and connect an I2C programmer to the same port. Attempt to write the characters “FFFF” over the entire EDID address range. 5. Disconnect the I2C programmer, reconnect computer #1 to the same port, and repeat step 3. 6. Reboot the TOE and repeat step 3. 7. Turn off the TOE and repeat step 3. 8. Restart the TOE and repeat step 3. 9. Disconnect computer #1 and repeat steps 2 to 8 with computer #2 on the same port. 10. Repeat steps 2 to 9 for a total of 20 EDID file captures. 11. Collect all 20 captured EDID files, compare them bit-by-bit, and verify that they are identical.
Execution Output	1. The evaluator ensured that the TOE was configured correctly. EDED reading and parsing software was running on two computers and a display was connected to the TOE. 2. The evaluator verified that the display showed video from computer #1. 3. The evaluator captured the TOE EDID content in the software on computer #1 and saved the file with a name that indicated capture time.

	4. The evaluator disconnected computer #1 and connected an I2C programmer to the same port. The evaluator attempted to write the charaters “FFFF” over the entire EDID address range but the EDID address change failed. 5. The evaluator disconnected the I2C programmer and reconnected computer #1 to the same port. 6. The evaluator rebooted the TOE and repeated step 3. 7. The evaluator turned off the TOE and repeated step 3. 8. The evaluator restarted the TOE and repeated step 3. 9. The evaluator disconnected computer #1 and repeated steps 2 to 8 with computer #2 on the same port. 10. The evaluator repeated steps 2 to 9 for to ensure 20 EDID files were captured. 11. The evaluator verified all 20 EDID files were identical by comparing them bit-by-bit.		
Pass/Fail Explanation	The evaluator confirms that that the TOE does not send data to different computers connected to the same TOE video interface over time. Overwriting the EDID address range was not possible. All EDID files were identical.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.22 FDP_CDS_EXT.1(1) Test 1

Objective	There are no test EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.23 FDP_CDS_EXT.1(2) Test 1

Objective	There are no test EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.24 FDP_FIL_EXT.1/KM Test 1

Item	*Data/Description*
Test ID	*FDP_FIL_EXT.1/KM – Test 1*
Objective	Perform the test steps in FDP_PDC_EXT.1 with all devices on the PSD KM blacklist and verify that they are rejected as expected.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, USBlyzer, Teledyne Lecroy USB Sniffer, Device Manager, MPOW Headset with USB Connector, Logitech USB Camera, HP Deskjet USB Printer, Identiv USB UA Device, Wireless LAN Dongle, BYEASY USB Hub, Dell Keyboard with Smart Card Reader, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Execution Steps	1. Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console.

	2. Attempt to connect the unauthorized device to the USB sniffer: • USB audio headset • USB camera • USB printer • USB user authentication device connected to a TOE keyboard/mouse peripheral interface • USB wireless LAN dongle 3. Power on the TOE. Verify the device is rejected. 4. Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again. 5. Verify the device is rejected. 6. Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical. 7. Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected, or the entire device is rejected.		
Execution Output	1. The evaluator ensured the TOE was powered off. USB analyzer software was running on the connected computer and a USB sniffer was connected to the TOE keyboard/mouse peripheral interface port. A real-time hardware information console was open on the computer. 2. The evaluator attempted to connect each unauthorized device to the USB sniffer: USB Audio headset, USB Camera, USB printer, USB user authentication device, and a USB wireless LAN dongle. 3. The evaluator powered on the TOE. The evaluator verified that the device was rejected using the USB protocol suite application. 4. The evaluator ensured the unauthorized device is disconnect from the USB sniffer, then reconnected. 5. The evaluator verified that the device is rejected using the USB protocol suite. The evaluator witnessed reset and suspend packets implicitly denying the unauthorized device. 6. The evaluator repeated steps 1 through 5 with a USB hub connected between the USB device and the USB sniffer. The devices remained rejected through the USB hub. 8. The evaluator repeated steps 1 through 6 with a composite device with non-HID device classes. The device was rejected.		
Pass/Fail Explanation	All devices on the PSD KM blacklist were tested and are rejected as expected. The evaluator confirms that the blacklist in place rejects all devices found in step 2. The evaluator confirmed through observation of the USB analyzer software that all blacklisted devices are rejected initially after power-on, after reconnecting, and whilst connected to a USB hub.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.25 FDP_FIL_EXT.1/KM Test 2

Objective	[Conditional: Perform this only if “configurable” is selected in FDP_FIL_EXT.1.1/KM] In the following steps the evaluator shall verify that whitelisted and blacklisted devices are treated correctly. Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance.

	Step 2: Connect to the TOE KM peripheral device interface a composite device which contains a HID class and a non-HID class. Step 3: Configure the TOE KM CDF to whitelist the composite device. Step 4: Verify that the HID-class part is accepted and that the non-HID class part is rejected through realtime device console and USB sniffer capture, or that the entire device is rejected. Step 5: Configure the TOE KM CDF to blacklist the device. Step 6: Verify that both the HID-class part and the non-HID class part is rejected through real-time device console and USB sniffer capture.
Evaluator Findings	"Configurable" has not been selected. Therefore, this evaluation activity is not applicable.
Verdict	Not Applicable

6.26 FDP_FIL_EXT.1/UA Test 1

Item	*Data/Description*		
Test ID	*FDP_FIL_EXT.1/UA – Test 1*		
Objective	Perform the test steps in FDP_PDC_EXT.1 with all devices on the PSD UA blacklist and verify that they are rejected as expected.		
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, USBlyzer, Device Manager, Identiv USB UA Device, BYEASY USB Hub, MPOW Headset with USB Connector, Logitech USB Camera, HP Deskjet USB Printer, Wireless LAN Dongle, Dell Keyboard with Smart Card Reader. Dell P2319H Monitor.		
Test Execution Steps	1. Ensure the TOE is powered off and connected to a computer. Run USB analyzer software and open the real-time hardware console on the connected computer and connect a USB sniffer to the unauthorized device. 2. Attempt to connect the unauthorized device via the USB sniffer to the TOE UA peripheral interface. 3. Power on the TOE. Verify the device is rejected. 4. Ensure the unauthorized device is disconnected from the TOE UA peripheral interface, then attempt to connect it again. 5. Verify the device is rejected. 6. Repeat steps 1-5 with a USB hub connected between the USB device and the USB sniffer and observe that the results are identical.		
Pass/Fail Explanation	The evaluator confirmed that all devices on the PSD UA blacklist are rejected as expected.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.27 FDP_FIL_EXT.1/UA Test 2

Item	*Data/Description*
Test ID	*FDP_FIL_EXT.1/UA – Test 2*
Objective	[Conditional: Perform this only if "configurable" is selected in FDP_FIL_EXT.1.1/UA]

	In the following steps the evaluator shall verify that whitelisted and blacklisted devices are treated correctly. Step 1: Configure the TOE UA CDF to whitelist an authorized user authentication device, connect it to the TOE UA peripheral device interface, and verify that the device is accepted through real-time device console and USB sniffer capture. Step 2: Configure the TOE UA CDF to blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture. Step 3: Attempt to configure the TOE UA CDF to both whitelist and blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture.		
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, Identiv USB UA Device, Device Manager, Dell P2319H Monitor.		
Test Execution Steps	1. Configure the TOE UA CDF to whitelist an authorized user authentication device, connect it to the TOE UA peripheral device interface, and verify that the device is accepted through real-time device console and USB sniffer capture. 2. Configure the TOE UA CDF to blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture. 3. Attempt to configure the TOE UA CDF to both whitelist and blacklist the device and verify that the device is rejected through real-time device console and USB sniffer capture.		
Execution Output	1. The evaluator configured the TOE UA CDF to whitelist an authorized user authentication device. The evaluator then connected the device to the TOE UA peripheral device interface and verified that the device was accepted after being whitelisted. 2. The evaluator configured the TOE UA CDF to blacklst the device and verified that the device was rejected after being blacklisted. 3. The evaluator attempted to configure the TOE UA CDF to both whitelist and blacklist the device. The evaluator verified that the device is rejected through real-time device console and the USB sniffer capture.		
Pass/Fail Explanation	The evaluator confirmed that whitelisted and blacklisted devices are treated correctly. When blacklisted, the device was rejected. When whitelisted, the device was accepted. When both blacklisted and whitelisted, the device was rejected.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.28 FDP_FIL_EXT.1/UA Test 3

Objective	Test 3 [Conditional – Perform this only if “fixed” is selected in FDP_FIL_EXT.1.1/UA] The evaluator shall examine the PSD UA whitelist and verify that all devices are authorized devices.
Evaluator Findings	“Configurable” has been selected, and therefore this evaluation activity is not applicable.
Verdict	Not Applicable

6.29 FDP_IPC_EXT.1 Test 1

Objective	Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.30 FDP_PDC_EXT.1 Test 1

Item	*Data/Description*				
Test ID	*FDP_PDC_EXT.1 – Test 1*				
Objective	The evaluator shall check the TOE and its supplied cables and accessories to ensure that there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.				
Test Equipment Used	N/A				
Test Execution Steps	1. Check the supplied cables and accessories to ensure there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.				
Pass/Fail Explanation	The evaluator confirms that all supplied cables and accessories contain no external wired interfaces. This excludes computer interfaces, peripheral device interfaces, and power interfaces.				
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH	SCAFP0004
Result	PASS	PASS	PASS	PASS	PASS

6.31 FDP_PDC_EXT.1 Test 2

Item	*Data/Description*				
Test ID	*FDP_PDC_EXT.1 – Test 2*				
Objective	The evaluator shall check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.				
Notes	• The evaluator confirms that the test execution steps were performed on all the units detailed in the units tested section. The same execution output was observed for each model tested. • Testing was performed on SC945DPH and SCAFP0004, but complete and full testing was performed on units SCM185DPH, SC845DPHC and SCMV245DPH.				
Test Execution Steps	1. Check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.				
Pass/Fail Explanation	The evaluator has checked the TOE for radio frequency certification information and verifies the TOE does not support wireless interfaces.				
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH	SCAFP0004
Result	PASS	PASS	PASS	PASS	PASS

6.32 FDP_PDC_EXT.1 Test 3

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1 – Test 3*
Objective	The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections (Appendix E). For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, or incompatibility of the device interface with the peripheral interface, and through no such device appearing in the real-time hardware information console. Step 1: Ensure the TOE is powered off. Open a real-time hardware information console on the connected computer. Step 2: Attempt to connect a USB mass storage device to the TOE peripheral interface. Step 3: Power on the TOE. Verify the device is rejected. Step 4: Ensure the USB mass storage device is disconnected, and then attempt to connect it to the TOE peripheral interface again. Step 5: Verify the device is rejected. Step 6: Power off the TOE. Connect an unauthorized USB device to a USB hub, and attempt to connect the USB hub to the TOE peripheral interface. Step 7: Power on the TOE. Verify the device is rejected. Step 8: Ensure the USB hub is disconnected, and then attempt to connect it to the TOE peripheral interface again. Step 9: Verify the device is rejected. Step 10: Power off the TOE. Attempt to connect any Personal System/2 (PS/2) device directly to the TOE peripheral interface. Step 11: Power on the TOE. Verify the device is rejected. Step 12: Ensure the PS/2 device is disconnected, and then attempt to connect it directly to the TOE peripheral interface again. Step 13: Verify the device is rejected.
Test Equipment Used	Device Manager, BYEASY USB Hub, PS/2 to USB Adapter, Perixx PS/2 Optical Mouse, HSL BADUSB, Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. Ensure the TOE is powered off. Open a real-time hardware information console on the connected computer. 2. Attempt to connect a USB mass storage device to the TOE peripheral interface. 3. Power on the TOE. Verify the device is rejected. 4. Ensure the USB mass storage device is disconnected, and then attempt to connect it to the TOE peripheral interface again. 5. Verify the device is rejected. 6. Power off the TOE. Connect an unauthorized USB device to a USB hub, and attempt to connect the USB hub to the TOE peripheral interface.

	7. Power on the TOE. Verify the device is rejected. 8. Ensure the USB hub is disconnected, and then attempt to connect it to the TOE peripheral interface again. 9. Verify the device is rejected. 10. Power off the TOE. Attempt to connect any Personal System/2 (PS/2) device directly to the TOE peripheral interface. 11. Power on the TOE. Verify the device is rejected. 12. Ensure the PS/2 device is disconnected, and then attempt to connect it directly to the TOE peripheral interface again. 13. Verify the device is rejected.			
Execution Output	1. The TOE was powered off. A real-time hardware information console application was running on the connected computer. 2. The evaluator connected a USB mass storage device to the TOE peripheral interface. 3. The TOE was powered on; the device was rejected. This was verified using device manager on the connected computer as well as the visual LED indicator on the front of the TOE. 4. The evaluator disconnected the USB mass storage device, then connected it to the TOE peripheral interface again. 5. The device was rejected. This was verified using device manager on the connected computer as well as the visual LED indicator on the front of the TOE. 6. The TOE was powered off. The evaluator connected an unauthorized USB device to a USB hub. Then the device was connected to the TOE peripheral interface again. 7. The TOE was powered on; the device was rejected. This was verified using device manager on the connected computer as well as the visual LED indicator on the front of the TOE. 8. The evaluator disconnected the USB hub, then connected it to the TOE peripheral interface again. 9. The device was rejected. This was verified using device manager on the connected computer as well as the visual LED indicator on the front of the TOE. 10. The TOE was powered on. The evaluator attempted to connect a PS/2 device directly to the TOE peripheral interface (The PS/2 device cannot be connected as the TOE contains no PS/2 ports). 11. The TOE was powered on; and the device was rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports). 12. The PS/2 device was disconnected; the evaluator attempted to connect it to the TOE peripheral interface again (The PS/2 device cannot be connected as the TOE contains no PS/2 ports). 14. The device was rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports).			
Pass/Fail Explanation	The evaluator confirmed that the TOE ports properly rejects unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections in (Appendix E). The output of the hardware console indicated a device rejection while unauthorized devices were connected and again across power cycling the TOE.			
Remote Control Used	SCAFP0004	SCAFP0004	SCAFP0004	SCAFP0004
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS	PASS

6.33 FDP_PDC_EXT.1 Test 1-AO

Item	*Data/Description*		
Test ID	*FDP_PDC_EXT.1/AO – Test 1*		
Objective	The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections. For this test, verify device rejection through TOE user indication in accordance with the operational user guidance or an immediate cessation of traffic following device detection or enumeration, or incompatibility of the device interface with the peripheral interface. Step 1: Ensure the TOE is powered off and audio analyzer software is running on the connected computer. Step 2: Connect an analog microphone to the TOE analog audio output peripheral interface. Step 3: Power on the TOE, speak loudly into the microphone from approximately one-inch distance, and verify no audio is present in the audio analyzer software. Step 4: Disconnect the microphone and reconnect it to the TOE peripheral interface. Step 5: Speak loudly into the microphone from approximately one-inch distance, and verify no audio is present in the audio analyzer software.		
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, TrueRTA, 3.5mm Microphone, 3.5mm Audio Splitter, MPOW Headset with USB Connector.		
Test Execution Steps	1. Ensure the TOE is powered off and audio analyzer software is running on the connected computer. 2. Connect an analog microphone to the TOE analog audio output peripheral interface. 3. Power on the TOE, speak loudly into the microphone from approximately one-inch distance, and verify no audio is present in the audio analyzer software. 4. Disconnect the microphone and reconnect it to the TOE peripheral interface. 5. Speak loudly into the microphone from approximately one-inch distance, and verify no audio is present in the audio analyzer software.		
Execution Output	1. The evaluator verified that the TOE was powered off and audio analyzer software was running on connected computer (LAB PC). 2. The evaluator verified that the analog microphone was connected to the TOE audio output peripheral interface. 3. The evaluator powered on the TOE and spoke loudly into the microphone. No audio was present in the audio analyzer software (LAB PC). 4. The evaluator disconnected the microphone and reconnected it to the TOE peripheral interface. 6. The evaluator spoke loudly into the microphone. No audio was present in the audio analyzer software (LAB PC).		
Pass/Fail Explanation	The evaluator confirmed that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.34 FDP_PDC_EXT.1 Test 1-KM

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1/KM – Test 1*
Objective	Test 1-KM: The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections. For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, no traffic captured on the USB sniffer or analyzer software other than NAK transactions or system messages, or incompatibility of the device interface with the peripheral interface. Also verify device rejection through examination of the USB sniffer or analyzer software for no traffic captured other than NAK transactions or system messages and through examination of the real-time hardware console for no display of new USB devices (recognized or not recognized). Repeat this test for each keyboard/mouse TOE peripheral interface. Perform steps 1-6 for each of the following unauthorized devices: • USB audio headset • USB camera • USB printer • USB user authentication device connected to a TOE keyboard/mouse peripheral interface • USB wireless LAN dongle Step 1: Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console. Step 2: Attempt to connect the unauthorized device to the USB sniffer. Step 3: Power on the TOE. Verify the device is rejected. Step 4: Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again. Step 5: Verify the device is rejected. Step 6: Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical. Step 7: Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected or the entire device is rejected.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, USBlyzer, Teledyne Lecroy USB Sniffer, MPOW Headset with USB Connector, Logitech USB Camera, HP Deskjet USB Printer, Identiv USB UA Device, Wireless LAN Dongle, BYEASY USB Hub, Dell

	Keyboard with Smart Card Reader, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor, Device Manager.		
Test Execution Steps	1. Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console. 2. Attempt to connect the unauthorized device to the USB sniffer: • USB Audio headset • USB Camera • USB Printer • USB user authentication device connected to a TOE K/M peripheral interface • USB wireless LAN dongle 3. Power on the TOE. Verify the device is rejected. 4. Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again. 5. Verify the device is rejected. 6. Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical. 7. Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected, or the entire device is rejected.		
Execution Output	1. The evaluator ensured the TOE was powered off. USB analyzer software was running on the connected computer and a USB sniffer was connected to the TOE keyboard/mouse peripheral interface port. A real-time hardware information console was open on the computer. 2. The evaluator attempted to connect each unauthorized device to the USB sniffer: USB Audio headset, USB Camera, USB printer, USB user authentication device, and a USB wireless LAN dongle. 3. The evaluator powered on the TOE. The evaluator verified that the device was rejected using the USB protocol suite application. 4. The evaluator ensured the unauthorized device is disconnect from the USB sniffer, then reconnected. 5. The evaluator verified that the device is rejected using the USB protocol suite. The evaluator witnessed reset and suspend packets implicitly denying the unauthorized device. 6. The evaluator repeated steps 1 through 5 with a USB hub connected between the USB device and the USB sniffer. The devices remained rejected through the USB hub. 8. The evaluator repeated steps 1 through 6 with a composite device with non-HID device classes. The device was rejected.		
Pass/Fail Explanation	The evaluator observed the output of the USB analyzer software and confirmed that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections. The devices listed in step 2 were all properly rejected including when attached to a USB hub.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.35 FDP_PDC_EXT.1 Test 2-KM

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1/KM – Test 2*
Objective	Test 2-KM: The evaluator shall verify that the TOE KM ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections. Repeat this test for each of the following four device types: • Barcode reader; • Keyboard or Keypad; • Mouse, Touchscreen, Trackpad, or Trackball; and • PS/2 to USB adapter (with a connected PS/2 keyboard or mouse). Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Run an instance of a text editor on a connected computer. Step 2: Ensure the TOE is powered off. Step 3: Connect the authorized device to the TOE peripheral interface. Step 4: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present. Step 5: Ensure the connected computer is selected and send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer. Step 6: Disconnect the authorized device, and then reconnect it to the TOE KM peripheral device interface. Step 7: Verify the TOE user indication described in the operational user guidance is not present. Step 8: Send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, Netum USB Barcode Reader, PS/2 to USB Adapter, Perixx Optical PS/2 Mouse, Dell P2319H Monitor.
Test Execution Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Run an instance of a text editor on a connected computer. 2. Ensure the TOE is powered off. 3. Connect the authorized device to the TOE peripheral interface: • Barcode reader; • Keyboard or Keypad; • Mouse, Touchscreen, Trackpad, or Trackball; and • PS/2 to USB adapter (with a connected PS/2 keyboard or mouse). 4. Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present.

	5. Ensure the connected computer is selected and send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer. 6. Disconnect the authorized device, and then reconnect it to the TOE KM peripheral device interface. 7. Verify the TOE user indication described in the operational user guidance is not present. 8. Send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer.		
Execution Output	1. The evaluator ensured the TOE and operational environment was configured; a text editor application was running on the connected computer. 2. The evaluator ensures the TOE was powered off. 3. The evaluator connected each authorized device to the TOE peripheral interface: Barcode reader, keyboard, mouse, and a PS/2 to USB adapter. 4. The TOE was powered on. The evaluator ensured the user indication was not present. 5. The evaluator ensured the connected computer is selected and sends input using the authorized device. The input is received into the text editor or on screen of the connected computer. 6. The evaluator disconnected the authorized device and then reconnected it to the TOE KM peripheral interface port. 7. The evaluator verified that the user indication was not present. 9. Input from the authorized device was present via text editor or on screen of the connected computer.		
Pass/Fail Explanation	The evaluator observed the output of the USB analyzer to confirm that the TOE KM ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections. The evaluator has confirmed that authorized devices were accepted by the TOE and the input was successfully received via the text editor.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.36 FDP_PDC_EXT.1 Test 1-UA

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1 – Test 1-UA*
Objective	Test 1-UA: Unauthorized Device Rejection [Conditional: Perform this test if “external” is selected in FDP_PDC_EXT.4.1] This test verifies that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections. For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, no traffic captured on the USB sniffer or analyzer software other than NAK transactions or system messages, or incompatibility of the device interface with the peripheral interface. Also verify device rejection through examination of the USB sniffer or analyzer software for no traffic captured other than NAK transactions or system messages and through examination of the

	real-time hardware console for no display of new USB devices (recognized or not recognized). Perform this test for an unauthorized device presenting itself as a composite device, a USB camera, a USB audio headset, a USB printer, a USB keyboard, a USB wireless dongle, and any device listed on the PSD UA blacklist. Repeat this for each user authentication TOE peripheral interface. Step 1: Ensure the TOE is powered off and connected to a computer. Run USB analyzer software and open the real-time hardware console on the connected computer, and connect a USB sniffer to the unauthorized device. Step 2: Attempt to connect the unauthorized device via the USB sniffer to the TOE UA peripheral interface. Step 3: Power on the TOE. Verify the device is rejected. Step 4: Ensure the unauthorized device is disconnected from the TOE UA peripheral interface, then attempt to connect it again. Step 5: Verify the device is rejected. Step 6: Repeat steps 1-5 with a USB hub connected between the USB device and the USB sniffer and observe that the results are identical.		
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, USBlyzer, Device Manager, Identiv USB UA Device, BYEASY USB Hub, MPOW Headset with USB Connector, Logitech USB Camera, HP Deskjet USB Printer, Wireless LAN Dongle, Dell Keyboard with Smart Card Reader, Dell P2319H Monitor.		
Test Execution Steps	1. TOE is powered off, hardware console application is running, and USB sniffer is connected to unauthorized device. 2. Unauthorized device connected to USB sniffer. 3. TOE is powered off. Device is rejected. 4. Disconnect then reconnect the device. 5. Device will be rejected. 6. Device will be rejected.		
Execution Output	1. The evaluator ensured the TOE was powered off, hardware console application was running, and USB sniffer was connected to an unauthorized device. 2. The evaluator attempted to connect the unauthorized device via the USB sniffer to the TOE UA peripheral interface. 3. The evaluatored ensured the TOE was powered on. The unauthorized device was sucessfully rejected. 4. The evaluator ensured the unauthorize device is disconnect from the TOE UA peripheral interface, then attempted to connect it again. 5. The evaluator verified the device was rejected by examining the USB sniffer. 7. The evaluator repeated step 1 – 5 with a USB hub connected between the USB device and USB sniffer. The evaluator verified that the results were identical and the unauthoized device was rejected.		
Pass/Fail Explanation	The evaluator confirmed using a USB sniffer that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.37 FDP_PDC_EXT.1 Test 2-UA

Item	*Data/Description*
Test ID	*FDP_PDC_EXT – Test 2*
Objective	Test 2-UA: Authorized Device Acceptance [Conditional: Perform this test if "external" is selected in FDP_PDC_EXT.4.1] This test verifies that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connection Policy. Perform this test for a USB device identified as User Authentication and any device listed on the PSD UA whitelist: Step 1: Ensure the TOE is powered off. Step 2: Connect the authorized device to the TOE peripheral interface. Step 3: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present. Step 4: Ensure the connected computer is selected and attempt to connect an authentication session. Verify that the authentication session is successfully connected on the connected computer. Step 5: Disconnect the authorized device, then reconnect it to the TOE peripheral interface. Step 6: Verify the TOE user indication described in the operational user guidance is not present. Step 7: Attempt to start an authentication session. Verify that the authentication session begins on the connected computer.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Identiv USB UA Device, Dell P2319H Monitor.
Test Execution Steps	1. Ensure the TOE is powered off. 2. Connect the authorized device to the TOE peripheral interface. 3. Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present. 4. Ensure the connected computer is selected and attempt to connect an authentication session. Verify that the authentication session is successfully connected on the connected computer. 5. Disconnect the authorized device, then reconnect it to the TOE peripheral interface. 6. Verify the TOE user indication described in the operational user guidance is not present. 7. Attempt to start an authentication session. Verify that the authentication session begins on the connected computer.
Execution Output	1. The evaluated ensured the TOE was powered off. 2. The evaluator connected the authorized device to the TOE peripheral inteface. 3. The evaluator powered on the TOE. The TOE user indication was not present. 4. The evaluator ensured the connected computer is selected and attempted to connect an authentication session. The evaluator verified the authentication session was successful on connected computer.

	5. The evaluator disconnected the authorized device, then reconnected it to the TOE peripheral interface. 6. The evaluator verified that the TOE user indication was not present. 8. The evaluator attempted to start and authentication session. The authentication session sucessfully begins on connected computer.		
Pass/Fail Explanation	The evaluator confirms that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connection Policy.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.38 FDP_PDC_EXT.1 Test 1-VI

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1 – Test 1*
Objective	Test 1-VI: The evaluator shall verify that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connections appendix in MOD_VI_V1.0. Repeat this test for each of the selected protocols in FDP_PDC_EXT.3.1/VI: Step 1: Connect the authorized device with an authorized protocol directly to a computer. Display any image on the device. Disconnect the device from the computer. Step 2: Configure the TOE and the Operational Environment in accordance with the operational guidance. Step 3: Ensure the TOE is powered off. Step 4: Connect the authorized device with an authorized protocol to the TOE peripheral interface. Step 5: Power on the TOE and verify the TOE user indication described in the operational user guidance is not present. Step 6: Ensure the connected computer is selected and verify that the device displays the same image as in step 1. Step 7: Disconnect the authorized device, then reconnect it to the TOE peripheral interface. Step 8: Verify the TOE user indication described in the operational user guidance is not present. Step 9: Verify that the device displays the same image as in step 1 and 6.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. Connect the authorized device with an authorized protocol directly to a computer. Display any image on the device. Disconnect the device from the computer. 2. Configure the TOE and the Operational Environment in accordance with the operational guidance. 3. Ensure the TOE is powered off. 4. Connect the authorized device with an authorized protocol to the TOE peripheral interface.

	5. Power on the TOE and verify user indication described in the operational user guidance is not present. 6. Ensure the connected computer is selected and verify that the device displays the same image as in step 1. 7. Disconnect the authorized device, then reconnect it to the TOE peripheral interface. 8. Verify the TOE user indication described in the operational user guidance is not present. 9. Verify that the device displays the same image as in step 1 and 6.		
Execution Output	1. The evaluator connected an authorized device with authorized protocol directly to a computer. An image was displayed on the device and then the device was disconnected from the computer. 2. The TOE was configured in accordance with the operational guidance. 3. The evaluator ensured the TOE was fully powered off. 4. The evaluator connected an authorized device with an authorized protocol to the TOE peripheral interface. 5. The evaluator powered on the TOE and verified that the user indication was not present. 6. The evaluator verified that the same image as step 1 is displayed. 7. The evaluator disconnected the authorized device then reconnected it to the TOE peripheral interface. 8. The evaluator verified that the user indication was not present. The evaluator verified that the device displays the same image as step 1 and 6.		
Pass/Fail Explanation	The evaluator confirms that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connections appendix in MOD_VI_V1.0.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.39 FDP_PDC_EXT.2/AO Test 1

Item	*Data/Description*
Test ID	*FDP_PDC_EXT – Test 2*
Objective	The evaluator shall verify that the TOE ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections. Repeat this test for each of the following devices: analog headphone, and analog speakers. Step 1: Ensure the TOE is powered off. Step 2: Connect the authorized device to the TOE peripheral interface. Step 3: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present. Step 4: Play an audio file on the connected computer and verify the sound is heard through the authorized device. Step 5: Disconnect the authorized device, then reconnect it to the TOE peripheral interface.

	Step 6: Verify the TOE user indication described in the operational user guidance is not present. Step 7: Play an audio file on the connected computer and verify the sound is heard through the authorized device.		
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, MPOW 3.5mm Headset, Edifier Multimedia Speaker.		
Test Execution Steps	1. Ensure the TOE is powered off. 2. Connect the authorized device to the TOE peripheral interface. 3. Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present. 4. Play an audio file on the connected computer and verify the sound is heard through the authorized device. 5. Disconnect the authorized device, then reconnect it to the TOE peripheral interface. 6. Verify the TOE user indication described in the operational user guidance is not present. 7. Play an audio file on the connected computer and verify the sound is heard through the authorized device.		
Execution Output	1. The evaluator verified that the TOE was powered off by unplugging the power cable. 2. The evaluator connected an authorized device (MPOW 3.5mm headset / Edifier Multimedia Speaker) to TOE peripheral interface. 3. The evaluator powered on the TOE and verified that the failure user indication was not present. 4. The evaluator played an audio file on the connected computer. Sound was audible through authorized device. 5. The evaluator dsconnectd the authorized device then reconnected it to the TOE peripheral interface. 6. The evaluator verified that The TOE user indication was not present. 7. The evaluator played an audio file on the connected computer. Sound was audible through the authorized device.		
Pass/Fail Explanation	The evaluator confirms that the TOE ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.40 FDP_PDC_EXT.2/KM Test 1

Objective	Testing of this component is performed through evaluation of FDP_PDC_EXT.1 Test 2 as specified in section 2.2.2.2 above. (See FDP_PDC_EXT.1.)
Evaluator Findings	Not Applicable. See FDP_PDC_EXT.1.
Verdict	Not Applicable

6.41 FDP_PDC_EXT.2/VI Test 1

Objective	Testing of this component is performed through evaluation of FDP_PDC_EXT.1 as specified in section 2.2.1.2 above. (See FDP_PDC_EXT.1.)
Evaluator Findings	Not Applicable. See FDP_PDC_EXT.1.
Verdict	Not Applicable

6.42 FDP_PDC_EXT.3/KM Test 1

Objective	Test activities for this SFR are covered under FDP_APC_EXT.1 tests 1-KM and 3-KM.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.43 FDP_PDC_EXT.2/UA Test 1

Objective	The EAs for this SFR are performed as part of activities for FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable. See FDP_PDC_EXT.1.
Verdict	Not Applicable

6.44 FDP_PDC_EXT.3/VI Test 1

Objective	Testing of this component is performed through evaluation of FDP_APC_EXT.1 as specified in section 2.2.1.1 above.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1/VI/
Verdict	Not Applicable

6.45 FDP_PDC_EXT.4 Test 1

Objective	There are no test evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.46 FDP_PUD_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FDP_PUD_EXT.1 – Test 1*
Objective	Step 1: Connect the amplified speakers directly to computer #1's analog audio output interface (typically green in color). Set the volume at the speakers to approximately 25%.

	Step 2: Connect the computer interface audio cable to the TOE audio output computer interface and computer #1's analog audio microphone input interface (typically pink in color) instead of the computer analog audio output interface. Step 4: Connect an open 3.5 millimeter stereo plug to the TOE analog audio peripheral interface. Step 5: Power up the TOE and ensure computer #1 is selected. Step 6: Measure the DC voltage of stereo plug from the TOE analog audio peripheral interface between the ground terminal and each one of the other two terminals (tip and ring) using a digital voltmeter. Step 7: Verify the voltage is 0.2 volts or less, ensuring there is no DC bias voltage supplied to the microphone.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Edifier Multimedia Speaker, Fluke True Digital Multimedia, Spliced 3.5mm Cable.
Test Execution Steps	1. Connect the amplified speakers directly to computer #1's analog audio output interface (typically green in color). Set the volume at the speakers to approximately 25%. 2. Connect the computer interface audio cable to the TOE audio output computer interface and computer #1's analog audio microphone input interface (typically pink in color) instead of the computer analog audio output interface. 3. Connect an open 3.5-millimetre stereo plug to the TOE analog audio peripheral interface. 4. Power up the TOE and ensure computer #1 is selected. 5. Measure the DC voltage of stereo plug from the TOE analog audio peripheral interface between the ground terminal and each one of the other two terminals (tip and ring) using a digital voltmeter. 6. Verify the voltage is 0.2 volts or less, ensuring there is no DC bias voltage supplied to the microphone.
Execution Output	1. The evaluator connected amplified speakers to computer #1's analog audio output interface and set the volume to 25%. 2. The evaluator connected the computer interface audio cable to the TOE audio output computer interface and computer #1's analog audio microphone input interface instead of the computer analog audio output interface. 3. The evaluator connected an open 3.5-mm stereo plug to the TOE analog audio peripheral interface. 4. The evaluator powered up the TOE and ensured Computer #1 was selected. 5. The evaluator measured the DC voltage of the stereo plug from the TOE analog audio peripheral interface between the ground terminal and each of the other two terminals using a digital voltmeter. 7. The evaluator verified that the voltage was below 0.2 volts, ensuring no C bias voltage is supplied to the microphone.
Pass/Fail Explanation	The evaluator confirmed that the TOE does not supply power to an unauthorized device connected to the analog audio output interface. The TOE cannot be

	configured to supply power to a device connected to the analog audio output interface.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.47 FDP_PWR_EXT.1 Test 1

Item	*Data/Description*		
Test ID	*FDP_PWR_EXT – Test 1*		
Objective	The evaluator shall perform the following test for each connected computer: Step 1: Ensure the power source is disconnected from the TOE. Step 2: Connect a USB sniffer between a TOE UA computer interface and its computer, attempt to turn on the TOE, and verify the TOE is not powered on, the user authentication device is not present in the real time hardware console, and no traffic is captured in the USB sniffer.		
Notes	• The evaluator confirms that the test execution steps were performed on all the units detailed in the units tested section. The same execution output was observed for each model tested.		
Testbed	#1		
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, Device Manager, Notepad, Identiv USB UA Device, Dell P2319H Monitor.		
Test Execution Steps	1. Ensure the power source is disconnected from the TOE. 2. Connect a USB sniffer between a TOE UA computer interface and its computer, attempt to turn on the TOE, and verify the TOE is not powered on, the user authentication device is not present in the real time hardware console, and no traffic is captured in the USB sniffer.		
Execution Output	1. The evaluator ensured the power source was disconnected from the TOE. 3. A USB sniffer was connected between a TOE UA computer interface and its computer. The TOE was attempted to be powered on. No user authentication device was present in the hardware console and no traffic was captured in the USB sniffer.		
Pass/Fail Explanation	The evaluator confirmed the above test was performed for each connected computer. No user authentication device is present, and no traffic was captured in the USB sniffer.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.48 FDP_RDR_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FDP_RDR_EXT.1 – Test 1*
Objective	The evaluator shall use a BadUSB, programmable keyboard, and/or USB Rubber Ducky as a malicious USB device to perform the following test: Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Ensure the TOE is powered off and connect a USB sniffer between the TOE and a computer. Open the real-time hardware information console.

	Step 2: Configure the malicious USB device as a HID-class device and to re-enumerate as a mass storage device. Step 3: Connect the malicious USB device to the TOE KM peripheral interface. Step 4: Power on the TOE and activate the re-enumeration after 1 minute. Step 5: Verify device rejection per TOE guidance, the cessation of traffic passed in the USB sniffer, and the absence of the device and any new devices in the information console. Step 6: Remove the malicious USB device and reconfigure as a HID-class device and to re-enumerate as a mass storage device. Step 7: Connect the malicious USB device to the TOE KM peripheral interface and activate the reenumeration after 1 minute. Step 8: Verify device rejection per TOE guidance, the cessation of traffic passed in the USB sniffer, and the absence of the device and any new devices in the information console.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Device Manager, HSL BADUSB, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Execution Steps	1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Ensure the TOE is powered off and connect a USB sniffer between the TOE and a computer. Open a real-time hardware information console. 2. Configure the malicious USB device as a HID-class device and to re-enumerate as a mass storage device. 3. Connect the malicious USB device to the TOE KM peripheral interface. 4. Power on the TOE and active the re-enumeration after 1 minute. 5. Verify device rejection per TOE guidance, the cessation traffic passed in the USB sniffer, and the absence of the device and any new device in the information console. 6. Remove the malicious USB device and reconfigure as a HID-class device and to re-enumerate as a mass storage device. 7. Connect the malicious USB device to the TOE KM peripheral interface and active the re-enumeration after 1 minute. 8. Verify device rejection per TOE guidance, the cessation of traffic passed in the USB sniffer, and the absence of the device and any new devices in the information console.
Execution Output	1. The evaluator ensured the TOE was powered off. A USB sniffer was connected between the TOE and a computer. A hardware information console was open on the selected computer. 2. The malicious USB device was configured as a HID-class device and then to re-enumerate as a mass storage device. The USB device was pre-programmed to replicate the two functions if the toggle switch on the device was set to the “middle” position. 3. The evaluator connected the USB Device to the TOE KM peripheral interface. 4. The TOE was powered on and re-enumeration was active after 1 minute. 5. The evaluator verified device rejected by the cessation of traffic passed to the USB sniffer and the absence of the device in hardware information console. 6. The evaluator removed the malicious USB device. The device was reconfigured as a HID-class device and then to re-enumerate as a mass storage device.

	7. The evaluator connected the USB Device to the TOE KM peripheral interface and re-enumeration was activated after 1 minute. 9. The evaluator verified device rejected by the cessation of traffic passed to the USB sniffer and the absence of the device in hardware information console.		
Pass/Fail Explanation	The evaluator configured the USB device accordingly and verified that the device was rejected appropriately. The TOE rejects the device and no new devices appear in the hardware console after re-enumeration.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.49 FDP_RIP_EXT.1 Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.50 FDP_RIP.1/KM Test 1

Objective	There are no test EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.51 FDP_RIP_EXT.2 Test 1

Item	*Data/Description*
Test ID	*FDP_RIP_EXT.2 – Test 1*
Objective	Step 1: Perform the TOE memory purge or restore factory defaults according to the guidance and verify that the TOE enters a desirable secure state. The evaluator shall check that the log record is not deleted if a logging function is supported by the TOE.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Objective Steps	1. Perform the TOE memory purge or restore factory defaults according to the guidance and verify that the TOE enters a desirable secure state. 2. The evaluator shall check that the log record is not deleted if a logging function is supported by the TOE.
Expected Output	1. The evaluator performs a reset to factory defaults according to guidance and verifies that the TOE enters a secure state. 2. The evaluator confirms that the one-time programmable, critical, and non-critical logging functions were not deleted as a result of the memory purge.
Execution Output	1. The evaluator performed a reset to factory default on the TOE using the administrative console and verified that the TOE entered a secure state. 2. The evaluator confirmed that the one-time programmable, critical, and non-critical logging functions were not deleted as a result of the memory purge.

Pass/Fail Explanation	The evaluator confirmed that the TOE provides a restore factory default setting feature and correctly restores the state of the TOE. The log record was not deleted.			
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS	PASS

6.52 FDP_SPR_EXT.1/DP Test 1

Objective	Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI and Test 4-VI.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.53 FDP_SPR_EXT.1/HDMI Test 1

Objective	Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI and Test 4-VI.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.54 FDP_SPR_EXT.1/USB Test 1

Objective	Testing for this SFR is covered under FDP_APC_EXT.1 Test 3-VI and Test 4-VI.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.55 FDP_SWI_EXT.1 Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.56 FDP_SWI_EXT.2(1) Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.57 FDP_SWI_EXT.2(2) Test 1

Objective	There are no test Evaluation Activities for this component.

Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.58 FDP_SWI_EXT.3 Test 1

Objective	The evaluator shall verify that the keyboard and mouse devices are always switched together to the same connected computer throughout testing in FDP_APC_EXT.1 in section 2.2.2.1 above. Tests for this SFR are performed in FDP_APC_EXT.1 test 1-KM in section 2.2.2.1 above.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1.
Verdict	Not Applicable

6.59 FDP_TER_EXT.1 Test 1

Objective	Testing for this component is performed as part of FDP_APC_EXT.1 test 2-UA.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1.
Verdict	Not Applicable

6.60 FDP_TER_EXT.2 Test 1

Objective	Testing for this component is performed as part of FDP_APC_EXT.1 test 2-UA.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1.
Verdict	Not Applicable

6.61 FDP_TER_EXT.3 Test 1

Objective	Testing for this component is performed as part of FDP_APC_EXT.1 test 2-UA.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1.
Verdict	Not Applicable

6.62 FDP_UAI_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FDP_UAI_EXT.1 – Test 1*
Objective	Test 1 This test verifies that UA functionality is not sent to other USB interfaces. Perform this test for each computer interface.

	Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a display directly to each connected computer. Run USB protocol analyzer software and open a real-time hardware information console and a text editor on each connected computer. Ensure an authorized user authentication device is connected. Perform steps 2-4 for each TOE USB peripheral interface other than UA. Step 2: Connect a USB sniffer to the TOE USB peripheral interface. Step 3: Connect an authentication session and verify no traffic is captured on the USB sniffer. Step 4: Disconnect the USB sniffer and the authentication session. Perform steps 5-7 for each TOE USB computer interface other than UA. Step 5: Connect a USB sniffer to the TOE USB computer interface and ensure that computer is selected. Step 6: Connect an authentication session and verify no traffic is captured on the USB sniffer. Step 7: Disconnect the USB sniffer and the authentication session. Step 8: Power down the TOE. Step 9: For each TOE USB interface (peripheral device and computer) other than UA, connect the USB sniffer and verify no traffic is captured.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, Device Manager, Notepad, Identiv USB UA Device, Dell P2319H Monitor.
Test Execution Steps	1. Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a display directly to each connected computer. Run USB protocol analyzer software and open a real-time hardware information console and a text editor on each connected computer. Ensure an authorized user authentication device is connected. 2. Connect a USB sniffer to the TOE USB peripheral interface. 3. Connect an authentication session and verify no traffic is captured on the USB sniffer. 4. Disconnect the USB sniffer and the authentication session. 5. Connect a USB sniffer to the TOE USB computer interface and ensure that computer is selected. 6. Connect an authentication session and verify no traffic is captured on the USB sniffer. 7. Disconnect the USB sniffer and the authentication session. 8. Power down the TOE. 9. For each TOE USB interface (peripheral device and computer) other than UA, connect the USB sniffer and verify no traffic is captured.
Execution Output	1. The evaluator ensured the TOE was correctly configured. A display was connected directly to each computer. The USB protocol, text editor and hardware information applications were all running on the computer. An authorized user authentication device was connected. 2. The USB sniffer was connected to peripheral interface.

	3. The evaluator connected an authentication session and verified that no USB traffic was captured. 4. The evaluator disconnected the USB sniffer and the authentication session. 5. The evaluator connected a USB sniffer to the TOE USB computer interface and ensured the computer was selected. 6. The evaluator connected an authentication session and verified that no USB traffic was captured. 7. The evaluated ensured the authentication session was closed and the USB sniffer was disconnected. 8. The evaluator ensured the TOE was powered down. 10. The evaluator ensured that for each TOE USB interface other than the UA, they connected the USB sniffer and verified that no USB traffic was captured.		
Pass/Fail Explanation	The evaluator confirmed that USB traffic from the UA is not sent to other USB interfaces.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.63 FDP_UAI_EXT.1 Test 2

Item	*Data/Description*
Test ID	*FDP_UAI_EXT.1 – Test 2*
Objective	[Conditional: Perform this test only if the TOE supports KM functionality.] This test verifies that KM functionality is not sent to UA interfaces. Perform this test while the TOE is powered on and powered off. Step 1: Connect a KM device to the TOE KM peripheral interface. Perform steps 2-3 for each TOE UA computer interface. Step 2: Connect a USB sniffer to the TOE UA computer interface. Step 3: Exercise the functions of the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM in MOD_KM_V1.0 and verify that no traffic is sent and captured on the USB sniffer. [Conditional: Perform steps 4-5 only if “external” is selected in FDP_PDC_EXT.4.1] Step 4: Disconnect the USB sniffer and connect it to the TOE UA peripheral device interface. Step 5: Exercise the functions of the peripheral device type(s) selected in FDP_PDC_EXT.3.1/KM in MOD_KM_V1.0 and verify that no traffic is sent and captured on the USB sniffer.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Execution Output	1. The evaluator connected a KM device to TOE KM interface. 2. A USB Sniffer was connected to TOE UA computer interface. 3. The evaluator exercised the functions of the peripheral device type and verified that no USB traffic was captured or sent. 4. The evaluator disconnected the USB sniffer and connected it to the TOE UA peripheral interface. 1. The evaluator exercised he functions of the peripheral device type and confirmed that no USB traffic was captured or sent.

Pass/Fail Explanation	The evaluator confirmed that USB traffic is not sent to UA interfaces.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.64 FDP_UAI_EXT.1 Test 3

Item	*Data/Description*
Test ID	*FDP_UAI_EXT – Test 3*
Objective	[Conditional: Perform this test only if the TOE supports video functionality and "USB Type-C with DisplayPort as alternate function" is selected in FDP_PDC_EXT.3.1/VI in MOD_VI_V1.0.] This test verifies that USB video functionality is not sent to UA interfaces. Perform this test while the TOE is powered on and powered off. Perform steps 1-3 for each TOE UA computer interface and TOE USB type-C video peripheral interface. Step 1: Connect a USB sniffer to the TOE UA computer interface. Step 2: Connect a monitor to the TOE USB type-C video peripheral interface and verify that no traffic is sent and captured on the USB sniffer. Step 3: Play a video on the selected computer and verify that no traffic is sent and captured on the USB sniffer. [Conditional: Perform steps 4-7 only if "external" is selected in FDP_PDC_EXT.4.1] Step 4: Disconnect the monitor. Step 5: Disconnect the USB sniffer and connect it to the TOE UA peripheral device interface. Step 6: Reconnect the monitor to the TOE USB type-C video peripheral interface and verify that no traffic is sent and captured on the USB sniffer. Step 7: Play a video on the selected computer and verify that no traffic is sent and captured on the USB sniffer.
Evaluator Findings	This test is not applicable to this configuration as no KVM uses USB type-C as a console video output.
Verdict	Not Applicable

6.65 FDP_UDF_EXT.1/AO Test 1

Item	*Data/Description*
Test ID	*FDP_UDF_EXT.1/AO – Test 1*
Objective	Note: Data is considered not to transit the TOE if no signal greater than 45 dB of attenuation at the specific audio frequency is received. The evaluator shall perform the following test: Step 1: Connect a computer to the TOE analog audio output peripheral interface, run its tone generator software, and run audio analyzer software on the connected computer. Step 2: Perform steps 3-6 for each TOE analog audio output peripheral interface.

	Step 3: For each connected computer, ensure it is selected, use the tone generator on the computer connected to the TOE analog audio output peripheral interface to generate the designated frequencies, and verify that the audio is not present on the selected computer's audio analyzer software. Step 4: Replace the selected computer with an oscilloscope and connect an external audio signal generator to the TOE analog audio output peripheral interface. Perform step 5 with the signal generator set to the following settings: • Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed; • Signal average to 0V (negative swing) Step 5: Set the signal generator to generate the designated frequencies, and verify the signal on the oscilloscope is 11.2 mV or less.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, TrueRTA, Rigol Waveform Audio Signal Generator, Tektronix Oscilloscope, Spliced 3.5mm Cable, Dell P2319H Monitor.
Test Execution Steps	1. Connect a computer to the TOE analog audio output peripheral interface, run its tone generator software, and run audio analyzer software on the connected computer. 2. Perform steps 3-6 for each TOE analog audio output peripheral interface. 3. For each connected computer, ensure it is selected, use the tone generator on the computer connected to the TOE analog audio output peripheral interface to generate the designated frequencies, and verify that the audio is not present on the selected computer's audio analyzer software. 4. Replace the selected computer with an oscilloscope and connect an external audio signal generator to the TOE analog audio output peripheral interface. Perform step 5 with the signal generator set to the following settings: • Pure sine wave around the average voltage of half output (positive signal only), with the output signal set to 2.00 V peak-to-peak, calibrating the signal with the oscilloscope as needed; • Signal average to 0V (negative swing) 5. Set the signal generator to generate the designated frequencies and verify the signal on the oscilloscope is 11.2 mV or less.
Execution Output	1. The evaluator ensured a computer was connected to TOE audio output peripheral interface (LAB PC) with tone generator software and audio analyzer software running on the connected computer (PC #1). 2. The evaluator ensured steps 3-6 were performed for each TOE analog audio peripheral interface. 3. The evaluator ensured that for each connected computer, it was selected The tone generator on the computer connected to the TOE analog audio output peripheral interface (LAB PC) was used to generate the designated frequencies. The evaluator verified that no audio was not present on the selected computer's audio analyzer software (PC #1). 4. The evaluator replaced the selected computer (PC #1) with an oscilloscope and connected an external audio signal generator (Rigol) to the TOE analog audio output peripheral interface. The evaluator ensured Step #5 was performed with the audio signal generator set to 0V (negative swing) and 2V peak-to-peak output signal.

	6. The evaluator generated the designated frequencies and verified the signal on the oscilloscope was less than 11.2 mV.		
Pass/Fail Explanation	The evaluator confirmed that the TOE audio output peripheral interface is unidirectional and no data can be routed from a connected peripheral back to a connected computer.		
Units Tested	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS

6.66 FDP_UDF_EXT.1/KM Test 1

Objective	Test activities for this SFR are covered under FDP_APC_EXT.1 test 3-KM.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.67 FDP_UDF_EXT.1/VI Test 1

Objective	This component is evaluated through evaluation of FDP_APC_EXT.1 as specified in section 2.2.1.1 above.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1.
Verdict	Not Applicable

6.68 FMT_MOF.1 Test 1

This test satisfies the EAs for FIA_UID.2, FIA_UAU.2, FMT_SMR.1.

Item	*Data/Description*
Test ID	*FMT_MOF.1 – Test 1*
Objective	Step 1: Set up the TOE to enable administrator access per applicable TOE administrative guidance. Verify that the TOE is in factory default format. Step 2: Attempt to set the initial administrator user name and password. Step 3: Logon as a valid administrator and perform all authorized administrative functions to assure the logon was successful. Step 4: Log off from the TOE. Step 5: Attempt to logon with an incorrect administrator name. Verify that the logon is failing as expected and that administrative functions are unavailable. Step 6: Attempt to access administrative functions while there is no logged on administrator. Verify that all attempts fail. Step 7: If the TOE provides multiple administrative roles, repeat this test for each defined role to ensure that the authorizations for each role are consistent with what is described in the operational guidance.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.

Test Execution Steps	1. Set up the TOE to enable administrator access per applicable TOE administrative guidance. Verify that the TOE is in factory default format. 2. Attempt to set the initial administrator username and password. 3. Logon as a valid administrator and perform all authorized administrative functions to assure the logon was successful. 4. Log off from the TOE. 5. Attempt to logon with an incorrect administrative name. Verify that the logon is failing as expected and that administrative functions are unavailable. 6. Attempt to access administrative functions while there is no logged-on administrator. Verify that all attempts fail. 7. If the TOE provides multiple administrative roles, repeat this test for each define role to ensure that the authorizations for each role are consistent with what is described in the operational guidance.			
Execution Output	1. The TOE was set to enable administrator access; The evaluator ensured the TOE was in factory default format. 2. The Initial administrator username and password was set through the administrator console. 3. The evaluator logged in as an administrator and performed all authorized administrative functions. 4. The evaluator logged off from the TOE. The TOE responded by ending the terminal session successfully. 5. The evaluator attempted to logon with an incorrect administrator name. Administrative functions were unavailable, and the logon fails. The TOE responds with providing the user the following text: "[sc]wrong user name. try again…". 6. The evaluator attempted to access administrator functions with no logged-on administrator, attempts to do so fail. The TOE responds with providing the user the following text: "[sc]wrong user name. try again…". 7. The evaluator repeated the test using multiple administrator roles. The authorizations for each role were consistent with that is described in the operational guidance.			
Pass/Fail Explanation	The evaluator confirmed that the administrative functions described in FMT_MOF.1.1 are only available to identified administrator.			
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS	PASS

6.69 FMT_SMF.1 Test 1

Item	*Data/Description*
Test ID	*FMT_SMF.1 – Test 1*
Objective	The evaluator shall test the TOE's ability to provide the management functions by configuring the TOE and testing each option assigned from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. Log into the TOE using administrative credentials and password. 2. Under the main operation page, select option "5" for reset to factory defaults.

	3. Ensure the “reset to factory default” management function is present and tested accordingly. 4. Under the main operation page, select option “4” for account management. 5. Ensure the “create administrative account” management function is present and tested accordingly. 6. Under the main operation page, select option “4” for account management. 7. Ensure the “change password” management function is present and tested accordingly. 8. Under the main operation page, select option “2” for configure DPP (Dedicated Peripheral Port). 9. Ensure the “modify configurable device filtration (CDF) list for authentication devices” management function is present and tested accordingly.			
Execution Output	1. Logged into TOE using administrative credentials and password 2. The evaluator was presented with different administrative function options. 3. The “reset to factory default” management function was present and resets the TOE to factory default settings. 4. The evaluator was presented with different administrative function options. 5. The “create administrate account” management function was present and created an administrative account on the TOE. 6. The evaluator was presented with different administrative function options. 7. The “change password” management function was present and changed the password for the selected administrator. 8. The evaluator was presented with different administrative function options. 9. The “modify configurable device filtration (CDF) list for authentication devices” management function was present and allowed the administrator to configure device filtration for authenticated devices.			
Pass/Fail Explanation	The evaluator confirmed that the TOE provides management functions described in the ST and guidance documents and has tested each option accordingly.			
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS	PASS

6.70 FPT_NTA_EXT.1 Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.71 FPT_PHP.1 Test 1

Item	*Data/Description*
Test ID	*FPT_PHP.1 – Test 1*
Objective	The evaluator shall verify, for each tamper evident seal or label affixed to the TOE enclosure and TOE remote controller (if applicable), that any attempts to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.
Test Equipment Used	N/A

Test Execution Steps	1. Removed the tamper evident seals from the TOE. 2. Removed the tamper evident seals from the Remote Control	
Pass/Fail Explanation	The evaluator confirmed that any attempt to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.	
Units Tested	SC945DPH	SCAFP0004
Result	PASS	PASS

6.72 FPT_PHP.1 Test 2

Item	*Data/Description*	
Test ID	*FPT_PHP.1 – Test 2*	
Objective	The evaluator shall verify that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.	
Test Equipment Used	N/A	
Test Execution Steps	1. Attempt to remove the tamper evident seals from the TOE without damaging the tampering indicators.	
Pass/Fail Explanation	The evaluator confirms that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.	
Units Tested	SC945DPH	SCAFP0004
Result	PASS	PASS

6.73 FPT_PHP.3 Test 1

Item	*Data/Description*
Test ID	*FPT_PHP.3 – Test 1*
Objective	In the following testing the evaluator shall attempt to gain physical access to the TOE internal circuitry (enough access to allow the insertion of tools to tamper with the internal circuitry). The TOE anti- tampering function is expected to trigger, causing an irreversible change to the TOE functionality. The evaluator then shall verify that the anti-tampering triggering provides the expected user indications and also disables the TOE. TOE disabling means that the user would not be able to use the TOE for any purpose – all peripheral devices and computers are isolated. Note that it is obvious that if the TOE was physically tampered with, then the attacker may easily circumvent the tamper indication means (for example cut the relevant TOE front panel wires). Nevertheless, the following test verifies that the user would be unable to ignore the TOE tampering indications and resume normal work. The evaluator shall perform the following steps: Step 1: [conditional: this step is applicable for TOEs having a remote controller] The evaluator shall attempt to open the PSD remote controller enclosure enough to gain access to its internal circuitry and observe that the TOE is both permanently disabled and provides the proper indication that it has been tampered with in accordance with the operational user guidance.

	Step 2: The evaluator shall attempt to open the PSD enclosure enough to gain access to its internal circuitry and observe that the TOE is both permanently disabled and provides the proper indication that it has been tampered with in accordance with the operational user guidance. Step 3: The evaluator shall attempt to access the TOE settings to reset the tampering state and verify that it is not possible to recover from the tampered state. Step 4: The evaluator shall acquire a copy of the TOE that has been previously tampered with. Step 5: The evaluator shall power on the TOE and verify that the tampering indicator is displayed.
Notes	• TD0583 applied.
Test Equipment Used	N/A
Test Execution Steps	1. [Conditional: this step is applicable for TOEs having a remote controller] The evaluator shall attempt to open the PSD remote controller enclosure enough to gain access to its internal circuitry and observe that the TOE is both permanently disabled and provides the proper indications that is has been tampered with in accordance with the operational user guidance. 2. The evaluator shall attempt to open the PSD enclosure enough to gain access to its internal circuitry and observe that the TOE is both permanently disabled and provides the proper indication that it has been tampered with in accordance with the operational user guidance. 3. The evaluator shall attempt to access the TOE settings to reset the tampering state and verify that it is not possible to recover from the tampered state. 4. The evaluator shall acquire a copy of the TOE that has been previously tampered with. 5. The evaluator shall power on the TOE and verify that the tampering indicator is displayed.
Execution Output	1. The evaluator removed the tamper proof seals from the remote control. The seals showed “VOID” to indicate the unit has been tampered with. Once the remote control had been opened the anti-tampering mechanism released and rendered the unit permanently disabled. The remote control displayed the proper visual indications using its LEDs to prove the unit had been tampered with. 2. The evaluator removed the tamper proof seals from PSD. The seals showed “VOID” to indicate the unit had been tampered with. Once the PSD had been opened the anti-tampering mechanism released and rendered the unit permanently disabled. The PSD displayed the proper visual indications using its LEDs to prove the unit had been tampered with. 3. The evaluator attempted to reset the tampering state by re-arming/resetting the anti-tampering trigger. The evaluator could not recover the PSD from its tampered state. 4. The evaluator had acquired a copy of the TOE that has been previously tampered with. 6. The evaluator confirms the tampering indicator on TOE is displayed, and the unit is rendered permanently disabled.

Pass/Fail Explanation	The evaluator confirms that the anti-tampering triggering provides the expected user indications and disables the TOE.	
Units Tested	SC945DPH	SCAFP0004
Result	PASS	PASS

6.74 FPT_STM.1 Test 1

Item	*Data/Description*			
Test ID	*FPT_STM.1 – Test 1*			
Objective	The evaluator shall test the TOE's ability to provide time stamps. It is expected that this test be performed in conjunction with FAU_GEN.1.			
Test Objective Steps	1. Log into the TOE using administrative credentials and password. 2. Under the main operation page, select option "6" for logs and events. 3. Select either option "1","2", or "3" to bring up logs and events with accompanying time stamps.			
Expected Output	1. Logged into TOE using administrative credentials and password 2. Select the correct menu to bring up logs and events. 3. Logs and events will be displayed with time stamps accompanying each incident.			
Execution Output	1. The evaluator logged into the TOE using the administrative console. Administrative credentials and password were provided for a successful log in. 2. The evaluator selected option six (6) to bring up the logs and events menu. 3. The evaluator confirmed logs and events were displayed with time stamps accompanying each incident.			
Pass/Fail Explanation	The evaluator confirmed that the TOE provides time stamps with each audit record.			
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS	PASS

6.75 FPT_TST.1(1) and FPT_TST.1(2) Test 1

This test satisfies the EAs for FPT_FLS_EXT.1(1) and FPT_FLS_EXT.1(2).

Item	*Data/Description*
Test ID	*FPT_TST.1 – Test 1*
Objective	The evaluator shall trigger the conditions specified in the TSS that are used to initiate TSF self-testing and verify that successful completion of the selftests can be determined by following the corresponding steps in the operational guidance.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.

Test Execution Steps	1. The TOE must be powered off, ensure the power cable is removed from the TOE before proceeding. 2. Firmly press any of the front panel buttons on the TOE while simultaneously plugging in the power cable. This will cause the unit to enter a self-test failure mode where the TOE will be powered on, but unusable. The front panel lights will continue to cycle between the computers connected but the TOE remains inoperable. 3. The evaluator shall ensure no video/keyboard/mouse is being output from the TOE while it is in self-test failure state.			
Execution Output	1. The TOE was powered off and the evaluator removed the power cable from the TOE before proceeding. 2. The evaluator connected the power cable to the TOE and observed the TOE perform a start-up self-test diagnostic for the following criteria: ○ Verification of the front panel push buttons – The evaluator confirmed the front panel push buttons retained their secure state and no tampering or damage was present on the push buttons. ○ (Not applicable to SCMV245DPH) Verification of the active anti-tampering functionality – The evaluator confirmed the chassis retained its secure state and no tampering of the TOE was present. This includes no anti-tampering switches being triggered and no anti-tampering stickers being damaged. ○ Verification of the integrity of the microcontroller firmware – The evaluator confirmed that the firmware is loaded onto the TOE during manufacturing as read-only firmware. Therefore, when the TOE performed its self-test diagnostic it is understood that a successful operational mode startup determines that no changes to the firmware have occurred. ○ Verification of computer port isolation – The evaluator confirmed during self-testing packets are sent to various interfaces and attempts are made to detect traffic on other interfaces. If any traffic is detected the test fails and the TOE enters a disabled state. Therefore, any successful power on into operational mode is deemed a pass for this portion of self-testing. 4. Upon completion of the self-testing diagnostics the TOE powered into operational mode and channel 1 was selected by default. The evaluator confirmed that all four verifications steps were successfully complete and self-testing diagnostics were performed.			
Pass/Fail Explanation	The evaluator confirmed that that successful completion of the self-tests can be determined by following the corresponding steps in operational guidance.			
Remote Control Used	SCAFP0004	SCAFP0004	SCAFP0004	SCAFP0004
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS	PASS

6.76 FPT_TST_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FPT_TST_EXT.1 – Test 1*

Objective	The evaluator shall cause a TOE self-test failure and verify that the TOE responds by disabling normal functions and provides proper indications to the user.			
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.			
Test Execution Steps	1. The TOE must be powered off, ensure the power cable is removed from the TOE before proceeding. 2. Firmly press any of the front panel buttons on the TOE while simultaneously plugging in the power cable. This will cause the unit to enter a Self-test failure mode where the TOE will be powered on, but unusable. The front panel lights will continue to cycle between the computers connected but the TOE remains inoperable. 3. The evaluator shall ensure no video/keyboard/mouse is being output from the TOE while it is in self-test failure state.			
Pass/Fail Explanation	The evaluator confirmed that the TOE does preform a self-test failure and that the TOE responds by disabling normal functions and provides proper indications to the user.			
Remote Control Used	SCAFP0004	SCAFP0004	SCAFP0004	SCAFP0004
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS	PASS

6.77 FTA_CIN_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FTA_CIN_EXT.1 – Test 1*
Objective	Step 1: The evaluator shall configure the TOE and its operational environment in accordance with the operational user guidance. Step 2: The evaluator shall select a connected computer and power down the TOE, then power up the TOE and verify that the expected selected computer is indicated in accordance with the TSS and that the connection is active. Step 3: The evaluator shall repeat this process for every possible selected TOE configuration. Step 4: [Conditional] If “upon reset button activation” is selected in FPT_TST.1.1, then the evaluator shall repeat this process for each TOE configuration using the reset function rather than power-down and powerup. Step 5: The evaluator shall verify that the TOE selected computer indications are always on (i.e., continuous) and fully visible to the TOE user. Step 6: [Conditional] If the TOE allows peripherals to have active interfaces with different computers at the same time, the evaluator shall verify that each permutation has its own selection indications. Step 7: [Conditional] If “a screen with dimming function” is selected, the evaluator shall verify that indications are visible at minimum brightness settings in standard room illumination conditions. Step 8: [Conditional] If ”multiple indicators which never display conflicting information” is selected, the evaluator shall verify that either all indicators reflect the same status at all times, or the indicator for the most recently used switching

	mechanism displays the correct switching status and that all other indicators display the correct status or no status.
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. The evaluator shall configure the TOE and its operational environment in accordance with the operational user guidance. 2. The evaluator shall select a connected computer and power down the TOE, then power up the TOE and verify that the expected selected computer is indicated in accordance with the TSS and that the connection is active. 3. The evaluator shall repeat this process for every possible selected TOE configuration. 4. [Conditional] If "*upon reset button activation*" is selected in FPT_TST.1.1, then the evaluator shall repeat this process for each TOE configuration using the reset function rather than power-down and power-up. 5. The evaluator shall verify that the TOE selected computer indications are always on (i.e., continuous) and fully visible to the TOE user. 6. [Conditional] If the TOE allows peripherals to have active interfaces with different computers at the same time, the evaluator shall verify that each permutation has its own selection indications. 7. [Conditional] If "*a screen with dimming function*" is selected, the evaluator shall verify that indications are visible at minimum brightness settings in standard room illumination conditions. 8. [Conditional] If "*multiple indicators which never display conflicting information*" is selected, the evaluator shall verify that either all indicators reflect the same status at all times, or the indicator for the most recently used switching mechanism displays the correct switching status and that all other indicators display the correct status or no status
Execution Output	1. The TOE and its operational environment have been configured in accordance with the operational user guidance. 2. A computer was selected, then the TOE was powered down. The TOE was then powered up and the evaluator verified that the expected selected computer was indicated in accordance with the TSS and that the connection was active. 3. This process was repeated for every possible selected TOE configuration. 4. "U*pon reset button activation*" was not selected in FPT_TST.1.1, therefore this step was not tested. 5. The selected computer indications on the TOE were always on and fully visible to the TOE user. 6. The TOE allowed peripherals to have active indications with different computers at the same time. 7. "A *screen with dimming function*" was not selected, therefore testing for this step is non-applicable. 8. The indicators always reflect the same status, or the indicator for the most recently used switching mechanism displays the correct switching status and that all other indicators display the correct status or no status.
Pass/Fail Explanation	The evaluator confirms the TOE properly indicates which computer connection is active on TOE power up. The evaluator also verifies the behavior of all indicators

	when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.			
Remote Control Used	SCAFP0004	SCAFP0004	SCAFP0004	SCAFP0004
Units Tested	SC945DPH	SCM185DPH	SC845DPHC	SCMV245DPH
Result	PASS	PASS	PASS	PASS

7 Security Assurance Requirements

7.1 ADV_FSP.1 Basic Functional Specification

7.1.1 ADV_FSP.1

7.1.1.1 ADV_FSP.1 Activity 1

Objective	There are no specific Evaluation Activities associated with these SARs. The Evaluation Activities listed in this PP are associated with the applicable SFRs; since these are directly associated with the SFRs, the tracing element ADV_FSP.1.2D is implicitly already done, and no additional documentation is necessary. The functional specification documentation is provided to support the evaluation activities described in Section 5.2 and other activities described for AGD, and ATE SARs. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other Evaluation Activities being performed. If the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.
Evaluator Findings	Sufficient interface information was available to perform the evaluation activities.
Verdict	Pass

7.2 AGD_OPE.1 Operational User Guidance

7.2.1 AGD_OPE.1

7.2.1.1 AGD_OPE.1 Activity 1

Objective	The operational user guidance does not have to be contained in a single document. Guidance to users and Administrators can be spread among documents or web pages. The developer should review the Evaluation Activities contained in Section 5.2 of this PP to ascertain the specifics of the guidance for which the evaluator will be checking. This will provide the necessary information for the preparation of acceptable guidance.
Evaluator Findings	The evaluator examined the guidance documents to perform this evaluation. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

7.3 AGD_PRE.1 Preparative Procedures

7.3.1 AGD_PRE.1

7.3.1.1 AGD_PRE.1 Activity 1

Objective	As with the operational user guidance, the developer should look to the Evaluation Activities contained in Section 5.2 of this PP to determine the required content with respect to preparative procedures.
Evaluator Findings	The evaluator examined the guidance documents to perform this evaluation. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

7.4 ALC Assurance Activities

7.4.1 ALC_CMC.1

7.4.1.1 ALC_CMC.1 Activity 1

Objective	The “evaluation evidence required by the SARs” in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance, the evaluator implicitly confirms the information required by this component.
Evaluator Findings	The ST was used to determine the identification of the TOE. This was also corroborated by the identification in the TOE user guidance documents. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

7.4.2 ALC_CMS.1

7.4.2.1 ALC_CMS.1 Activity 1

Objective	Given the scope of the TOE and its associated evaluation evidence requirements, this component’s Evaluation Activities are covered by the Evaluation Activities listed for ALC_CMC.1.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

7.5 ATE_IND.1 Independent Testing – Conformance

7.5.1 ATE_IND.1

7.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP’s Evaluation Activities. While it is not necessary to have one test case per test listed in an Evaluation Activity, the evaluator must document in the test plan that each applicable testing requirement in the PP is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test equipment or tools. For each piece of equipment or tool, an argument (not just an

	assertion) should be provided that the equipment or tool will not adversely affect the performance of the functionality by the TOE and its platform. The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.
Evaluator Findings	The evaluator created a test plan and executed all the tests in the test plan. The results of all the testing are included in the test plan. Based on this document, this evaluation activity is considered satisfied.
Verdict	Pass

7.6 AVA_VAN.1 Vulnerability Survey

7.6.1 AVA_VAN.1

7.6.1.1 AVA_VAN.1 Activity 1

Objective	As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in peripheral sharing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.
Evaluator Findings	The evaluator documented the 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. The terms used to search within the previous websites are several combinations of the following words: Vertiv, Vertiv KVM, Vertiv Firmware, Firmware Version 44444-E7E7, Vertiv Peripheral Sharing Device, SCM185DPH, SC845DPHC, SCMV245DPH, SC945DPHC, SC845DPH, SCM145DPH, SC985DPH, SCMV285DPH, SC945DPH, SCAFP0004, Cybex, NAK transaction, SYNC Signal, HPD signal, EDID traffic, ARC Signal, HDCP signal, USB HID traffic and STMicroelectronics 32-Bit 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. • National Vulnerability Database: https://nvd.nist.gov/vuln/search • Vertiv Support: https://www.vertiv.com/en-us/support/ • Generic Internet Search: https://google.com

	The search was performed on May 25, 2021. 1. No current vulnerabilities were found. The term “Vertiv” returned 3 matches for a UMG-4000 product which were found not to be relevant to the TOE. The term “NAK transaction” returned 3 matches for non-TOE products with a DHCP protocol-specific vulnerability. The TOE is not a networked device. The term “SYNC signal” returned 5 matches that are not relevant to the TOE technology type. The term “EDID traffic” returned 10 results which were not relevant to the TOE technology type. The term “ARC signal” returned 69 results, none of which were found to be relevant to the TOE technology type. The term “HDCP signal” returned 16 results. All but CVE-2001-0903 were not applicable to the TOE technology type. CVE-2001-0903 is over 20 years old, with little detail available on exploitability. It is the evaluator’s opinion that the TOE is not uniquely exploitable as it is not a networked device. The vulnerability is only exploitable remotely, while the TOE is only accessible locally. The term “STMicroelectronics 32-bit” did not return any results. The evaluator augmented this search with the specific proprietary system controller part numbers utilized in each TOE model and also found no results. In researching known vulnerabilities on on similar STMicroelectronics controllers, it was found that any exploits would require a physical attacker with access to the interior of the unit, which would be mitigated by the anti-tamper mechanisms available in the TOE. No other search terms provided any potential matches. 2. No current vulnerabilities were found. 3. No current vulnerabilities were found. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

8 Conclusion

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

9 Evaluation Evidence

- [ST] Vertiv CYBEX™ SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM145DPH, SCM185DPH, SC985DPH, SCMV245DPH, SCMV285DPH Firmware Version 44444-E7E7 Peripheral Sharing Devices Security Target, v1.29, June 1, 2022
- [Isol] Vertiv CYBEX™ SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM145DPH, SCM185DPH, SC985DPH, SCMV245DPH, SCMV285DPH Firmware Version 44444-E7E7 Peripheral Sharing Devices Isolation Document, Version 1.10, May 28, 2022
- [CC_Supp] Vertiv CYBEX™ SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM145DPH, SCM185DPH, SC985DPH, SCMV245DPH, SCMV285DPH Firmware Version 44444-E7E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 1.7, May 28, 2022
- [Tech_Bull] Vertiv CYBEX™ SC/SCM Switching System Additional Operations and Configuration Technical Bulletin, 590-1741-501B
- [2282] CYBEX™ SC SERIES SECURE SWITCHES SC800/900DPH, SC800/900DVI, and SCKM100PP4 Quick Install Guide, 590-2282-501B
- [2284] CYBEX™ SC Series Secure Switches SC800DPHC/SC900DPHC Quick Install Guide, 590-2284-501B
- [2306] CYBEX™ SC Series Secure Switches SCM100DPH Desktop Matrix Quick Install Guide, 590-2306-501A
- [2307] CYBEX™ SC Series Secure Switches SCMV200DPH Multiviewer Quick Install Guide, 590-2307-501B
- [Testplan] Evaluation Test Plan for Vertiv CYBEX™ SC845DPH, SC945DPH, SC845DPHC, SC945DPHC, SCM145DPH, SCM185DPH, SC985DPH, SCMV245DPH, SCMV285DPH Firmware Version 44444-E7E7 Peripheral Sharing Devices, version 1.2, May 28, 2022

10 References

- [PP_PSD_V4.0] Protection Profile for Peripheral Sharing Device, July 19, 2019
- [MOD_AO_V1.0] PP-Module for Analog Audio Output Devices, July 19, 2019
- [MOD_KM_V1.0] PP-Module for Keyboard/Mouse Devices, July 19, 2019
- [MOD_UA_V1.0] PP-Module for User Authentication Devices, July 19, 2019
- [MOD_VI_V1.0] PP-Module for Video/Display, July 19, 2019
- [CFG_PSD_AO-KM-UA-VI_v1.0] PP-Configuration for Peripheral Sharing Device, Analog Audio Output Devices, Keyboard/Mouse Devices, User Authentication Devices, and Video/Display Devices, July 19, 2019

End of Document