

HONOLULU RAIL TRANSIT PROJECT

CORE SYSTEMS CONTRACT

COMMUNICATIONS SYSTEM

Security System: Access Control System (ACS) Operations Manual

PBS Code 4C
ABS Code C0
Location P00
Phase Code WP
Type X

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 1 of 430	

HRH DOCUMENT ISSUE

Date	XX/XX/XXXX

	Name and Surname	Designation
Approver		
Authorizer		

SUPPLIER DOCUMENT ISSUE

Date	XX/XX/XXXX



1001 Bishop Street
Ste 1503
Honolulu, HI 96813

	Name and Surname	Designation
Author	Stephen W. Mitchell	Technical Writer
Verifier	Daniel McNamee	Subject Matter Expert
	Marc Guenther	Subject Matter Expert

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 2 of 430

Traceability of Revisions

Revision	Date	Author	Approver	Authorizer	Revision Description
1.00	04/12/2020	Stephen W. Mitchell	Daniel McNamee	Nokia TBD	Final Draft for peer review and approval

DRAFT

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 3 of 430

Contents

LIST OF FIGURES	ERROR! BOOKMARK NOT DEFINED.
LIST OF TABLES	10
LIST OF APPENDICES	ERROR! BOOKMARK NOT DEFINED.
1 SCOPE	16
1.1 PURPOSE	16
1.2 APPLICABILITY	16
1.3 REFERENCE DOCUMENTS	17
1.3.1 Contractual Reference Documents	17
1.3.2 Project Reference Documents	17
1.3.3 International, National, and Local Reference Standards.....	18
1.4 TERMS, ACRONYMS, AND ABBREVIATIONS	19
1.5 DESCRIPTION OF CHANGES	22
1.6 DOCUMENT ORGANIZATION	22
1.6.1 HART ACS Operations Manual Organization	22
1.6.2 HART Communications System Operations and Maintenance Manuals	22
2 HART ACS	24
2.1 ACS ARCHITECTURE.....	24
2.1.1 Servers.....	29
2.1.2 Workstations.....	29
2.2 ACS HARDWARE.....	41
2.2.1 Access Card - HID 1386-LGGMN ISOProx II	41
2.2.2 Proximity Card Reader - HID Proximity Card System 1.....	42
2.2.3 SmartCard Reader - HID 920P MultiClass SE Readers.....	42
2.2.4 In/Out Module - Genetec Mercury Security MR-16IN I/O Module.....	44
2.2.5 In/Out Module - Genetec Mercury Security MR-16OUT Module.....	45
2.2.6 In/Out Module - Genetec Mercury Security MR-52 I/O Module	47
2.2.7 Telephone Entry Pad - Ameristar Gate 1837AGS.....	48
2.2.8 Request to Exit Detector and TP160 Trim Plates - Bosch DS150i.....	51
2.2.9 Sliding Shelf/Tray - Atlas Sound VTD1 16.....	52
2.2.10 Recessed Steel Door Contact - GE 1076D	52
2.2.11 Industrial Surface Mount Contact - Sentrol 1045 Position Sensors	53
2.2.12 Lock Box - Knox Box Bosch 3262	54
2.2.13 Key Switch - Camden CM1170-7024	54
2.2.14 Magnetic Contacts: Overhead Door - GE 2200A-L.....	55
2.2.15 Magnetic Contacts: Heavy Duty - Sentrol 2105.....	56
2.2.16 Push Button Exit Control - DynaLOCK 6270	57
2.2.17 IP Video Storage - BCDVideo BCD360V8.....	57
2.2.18 Motion Detector - Bosch ISC-CDL1 & B328	58
2.2.19 DC Rack Mount ACS Power Supply - Altronix R615DC1016.....	60
2.2.20 Rack Mount Access Power Controller - Altronix Maximal 33RD	61
2.2.21 Rackmount Server - BCDVideo BCD320E8-M-SAS-MP-C	61
2.2.22 Rackmount Server - BCDVideo BCD104-170-MP-C	61
2.2.23 Rack Mount DC Power Supply - AlarmSaf RM-PS5-MD-UL	62
2.2.24 Surface Mount Magnetic Contact - GE 2507A	64

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 4 of 430

2.2.25	Surface Mount Magnetic Contact - GE 2507AD.....	65
2.2.26	Digital Loop Protector - EPS 3416D.....	66
2.2.27	Preformed Vehicle Detection Loop - EPS PFL46	67
2.2.28	Pedestal - CEO 72-9C-D and LANDO-KY-20x14E	68
2.2.29	Lockable Drawer - Rack Solutions 2U 162-920	69
2.2.30	Glass Break Detector - Honeywell FlexGuard FG-730.....	70
2.2.31	Instrumentation Cable - Exane Firewall LSZH Type TC	71
2.3	ACS FIELD COMPONENTS.....	72
2.3.1	ACS/IDS Panel	72
2.3.2	ACS/IDS Input Boards.....	72
2.3.3	ACS/IDS Output Boards.....	73
2.3.4	ACS/IDS Door Interface.....	73
2.3.5	ACS/IDS Card Reader.....	73
2.3.6	Intrusion Alarm Sensors (Contacts).....	73
2.3.7	Traffic Loop Detector	73
2.3.8	Intrusion Alarm Panel	74
2.3.9	Intercom.....	74
2.3.10	Knox Box	74
2.4	ACS SOFTWARE - GENETEC SECURITY CENTER.....	74
2.4.1	Genetec Synergis	75
3	GENETEC SYNERGIS	78
3.1	SECURITY CENTER.....	78
3.1.1	Security Center Architecture.....	80
3.1.2	How the Security Center is Organized	81
3.2	INSTALLATION	82
3.2.1	Server Installation	82
3.2.2	Client Workstation Installation.....	82
3.3	QUICKSTART GUIDE.....	87
3.3.1	Log On	87
3.3.2	Log Off.....	92
3.4	SYSTEM ROLES	92
3.4.1	Directory Role	93
3.4.2	Archiver Role	96
3.4.3	Access Manager Role	96
3.4.4	Media Router Role	97
3.4.5	Zone Manager Role	97
3.4.6	Report Manager Role	97
3.4.7	Health Monitor Role.....	97
3.4.8	Map Manager Role.....	97
3.4.9	Web-Based SDK Role.....	97
3.4.10	Plugin Roles	97
3.4.11	Role Failover.....	98
3.4.12	Deactivate and Activate Roles	102
3.4.13	Move Roles to Other Servers	102
3.4.14	Connect Roles to Remote Database Servers	102
3.5	ACCESS CONTROL.....	104

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 5 of 430

3.5.1	Access Control Units	104
3.5.2	Access Control Entities	106
3.5.3	Access Controllers	111
3.5.4	Access Managers	112
3.5.5	Access Manager and Access Logic	114
3.5.6	Access Control Task	115
3.6	ACCESS RULES	116
3.6.1	Assign Access Rules to Cardholders	118
3.6.2	Assign Temporary Access Rules to Cardholders	120
3.6.3	Identify who Is Granted Access to Doors	121
3.6.4	Identify Who is Granted/Denied Access at Access Points	121
3.6.5	Identify Which Entities Are Affected by Access Rules	122
3.6.6	Enable External Access Control Devices	123
3.6.7	Investigate Events Related to Access Control Units	123
3.6.8	View I/O Configuration of Access Control Units	124
3.6.9	Test Cardholder Access Rights	125
3.6.10	Test Access Rules at Doors	125
3.6.11	Optional Access Rules	126
3.7	CARDHOLDER MANAGEMENT	127
3.7.1	Cardholders	128
3.7.2	Cardholder Groups	149
3.7.3	Receive Notifications When Cardholders Are Expiring	150
3.8	CREDENTIALS	151
3.8.1	Credential Management	151
3.8.2	Credentials – Access Control Task	151
3.8.3	Credentials – Access Management Task	152
3.8.4	Unused Credential and Cardholder Expiration Field	153
3.8.5	Search Unused Credentials and Cardholders	154
3.8.6	Credential Access Control	154
3.8.7	Credential Management Task	155
3.8.8	Credential Enrollment Methods	156
3.8.9	Enroll Credentials Multiple Automatically	157
3.8.10	Enroll Multiple Credentials Manually	158
3.8.11	Create Credentials	160
3.8.12	Respond to Credential Card Request	164
3.8.13	Investigate Request History of Credential Card	165
3.8.14	Report Pane Columns for the Credential Request History Task	166
3.8.15	Investigate Credential Events	166
3.8.16	Report Pane Columns for the Credential Activities Task	167
3.8.17	View Credential Properties of Cardholders	167
3.8.18	Report Pane Columns for the Credential Configuration Task	168
3.8.19	Search for Credentials	169
3.8.20	Report Pane Columns for the Credential Management Task	170
3.9	AREAS AND DOORS	170
3.9.1	Allow Access through Doors	172
3.9.2	Prevent Access through Doors	173
3.9.3	Investigate Area Events	174
3.9.4	Report Pane Columns for the Area Activities Task	174

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 6 of 430

3.9.5	Investigate Door Events.....	175
3.9.6	Report Pane Columns for the Door Activities Task.....	176
3.9.7	Identify Who is Granted/Denied Access at Access Points	176
3.9.8	Report Pane Columns for the Cardholder Access Rights Task	177
3.9.9	Identify Who is Granted Access to Doors.....	177
3.9.10	Report Pane Columns for the Door Troubleshooter Task	177
3.9.11	Identify Entities Affected by Access Rules.....	178
3.9.12	Report Pane Columns for the Access Rule Configuration Task	178
3.10	USER MANAGEMENT	179
3.10.1	User Properties.....	179
3.10.2	User Privileges.....	179
3.10.3	Unconfigured Users	180
3.10.4	Remote Control.....	181
3.10.5	User Groups	181
3.10.6	Resolve Conflicting Privileges.....	182
3.10.7	Users.....	182
3.10.8	User Groups	188
3.10.9	Privileges.....	192
3.11	ADDITIONAL CONFIGURATIONS.....	198
3.11.1	Areas.....	199
3.11.2	Schedule Management.....	206
3.11.3	Event Handling	219
3.11.4	Zones	239
3.11.5	Advanced Access Control.....	260
3.11.6	Badge Designer	317
3.12	ALARMS	326
3.12.1	How Alarms Display in the Security Desk Canvas	326
3.12.2	Enable Alarm Monitoring in the Monitoring Task	327
3.12.3	Alarm Information Available When Monitoring Alarms.....	328
3.12.4	Mute Repeated Alarm Sounds	329
3.12.5	Forward Alarms to Other Users Automatically	329
3.12.6	Forward Alarms to Other Users Manually.....	330
3.12.7	Alarm Priority.....	330
3.12.8	Video Recording on Alarms	330
3.12.9	Select Video Display Options for Alarms.....	330
3.12.10	Setting Optional Alarm Properties.....	332
3.12.11	Troubleshoot Alarms not Received.....	333
3.12.12	Set Up Alarms Using Event-to-Actions.....	333
3.12.13	Event Types That Can Require Acknowledgement Conditions.....	334
3.12.14	Alarm Acknowledgement Conditions.....	335
3.12.15	Acknowledging Alarms.....	336
3.12.16	Clear Source Condition.....	337
3.12.17	Incident Report Requirement	337
3.12.18	Receiving Alarms	338
3.12.19	Alternative Display Mode.....	338
3.12.20	Popup Alarm Display	339
3.12.21	Grouping Alarms	339
3.12.22	Server Alarm Trigger.....	341

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 7 of 430

3.12.23	Trigger an Alarm	344
3.12.24	Alarm Options	345
3.12.25	Alarm Privileges	346
3.12.26	Customize Alarm Behavior	347
3.12.27	Alarm Report	348
3.12.28	Report Pane Columns for the Alarm Report Task	349
3.12.29	Operational Alarms	350
3.12.30	Genetec Alarms, Incident and Threat Levels	352
3.12.31	Investigating Current and Past Alarms	353
3.13	REPORTS	354
3.13.1	Reporting Task Workspace	354
3.13.2	About Visual Reports	356
3.13.3	Generate a Report	360
3.13.4	Export a Generated Report	362
3.13.5	Generating Visual Reports	363
3.13.6	Generate and Save a Report	365
3.13.7	Customize the Report Pane	366
3.13.8	Customize Report Behavior	367
3.13.9	Set Maximum Report Results for Automated Reports	368
3.14	SYSTEM TOOLS	368
3.14.1	Access Troubleshooter Tool	368
3.14.2	Unit Enrollment Tool	369
3.14.3	Unit Replacement Tool	371
3.14.4	Replace Access Control Units	373
3.14.5	Move Unit Tool	374
3.14.6	Copy Config Tool	375
3.14.7	Upgrade Firmware	378
3.15	REPORTS	382
3.15.1	Schedule Routine Reports	385
3.16	NORMAL OPERATIONS	389
3.17	DEGRADED OPERATIONS	389
3.17.1	Cloud Link is Working but Server is Down	390
3.17.2	Inability to View System Messages	390
3.17.3	Inability to View Availability of Entities	391
3.17.4	SQL Server/Database Failure	391
3.17.5	Workstation Failure	392
3.17.6	Monitor Failure	392
3.17.7	HART Switchover from OCC to BOCC	392
3.18	EMERGENCY OPERATIONS	393
APPENDIX A.	ALARM LIST	394
APPENDIX B.	BILL OF MATERIALS	395
APPENDIX C.	SPARE PARTS LIST	403
APPENDIX D.	PRODUCT TREE AND ASSET LIST	405
APPENDIX E.	DATA SHEETS	406
APPENDIX F.	LICENSES	408

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 8 of 430

APPENDIX G.	WARRANTIES AND TECHNICAL SUPPORT	409
APPENDIX H.	OEM USER MANUALS	414
APPENDIX I.	TYPICAL LAYOUTS AND INSTALLATION DRAWINGS	415
APPENDIX J.	SYSTEM BLOCK DIAGRAMS	416
APPENDIX K.	SOFTWARE REQUIREMENTS	417
K1.	SOFTWARE REQUIREMENTS	417
K2.	WORKSTATION HARDWARE REQUIREMENTS	418
K3.	MAXIMUM NUMBER OF CAMERAS VIEWED PER CLIENT TYPE	418
K4.	PERFORMANCE BENCHMARK FOR HEVC (H.265)	420
K5.	MAXIMUM NUMBER OF CAMERAS AND READERS PER SERVER TYPE	420
APPENDIX L.	SOFTWARE RELEASE NOTES & LIFECYCLE DATA	421
L.1	PRODUCT LIFECYCLE	421
L.2	SECURITY CENTER LIFECYCLE RELEASE TRACKS	421
L.3	RELEASE TYPES	421
L.4	LIFECYCLE STAGES	422
L.5	PRODUCT LIFECYCLE POLICY SUMMARY	424
L.6	PRODUCT LIFECYCLE TIMELINE	425
L.7	SECURITY CENTER ADD-ON	427
APPENDIX M.	CERTIFICATES/DECLARATION OF CONFORMITY (DOC) CERTIFICATES	429
APPENDIX N.	REFERENCE TEST DATA	430

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 9 of 430

List of Figures

Figure 1. Organization of HART ICCS Security System by Manual	16
Figure 2. ACS Operations Manual Organization	22
Figure 3. HART ACS/IDS Architecture	25
Figure 4. ACS: Typical Station Layout	26
Figure 5. ACS/IDS Architecture for OCC, BOCC, MS , TPSS and GBS	27
Figure 6. ACS/IDS Architecture for Stations or Buildings	28
Figure 7. ACS/IDS Device Deployment	28
Figure 8. BCDVideo BCD230T	30
Figure 9. BCDVideo BCD230T Badge Printer	31
Figure 10. ID Badge Camera - 20K758USB-SYS.....	35
Figure 11. Signature Pad - Topaz Systems SigLit.....	36
Figure 12. HP LaserJet Enterprise 700 M712xh Printer	38
Figure 13. Access Card - HID 1386-LGGMN ISOProx II.....	41
Figure 14. SmartCard Reader - HID 920P MultiClass SE Readers.....	42
Figure 15. In/Out Module - Genetec Mercury Security MR-16IN I/O Module	44
Figure 16. In/Out Module - Genetec Mercury Security MR-16OUT Module.....	46
Figure 17. In/Out Module - Genetec Mercury Security MR-52 I/O Module.....	47
Figure 18. Telephone Entry - Ameristar Gate 1837AGS	48
Figure 19. Request to Exit Detector and TP160 Trim Plates - Bosch DS150i.....	51
Figure 20. Sliding Shelf/Tray - Atlas Sound VTD1 16.....	52
Figure 21. Recessed Steel Door Contact - GE 1076D	52
Figure 22. Industrial Surface Mount Contact - Sentrol 1045 Position Sensors	53
Figure 23. Lock Box - Knox Box Bosch 3262	54
Figure 24. Key Switch - Camden CM1170-7024	54
Figure 25. Magnetic Contacts: Overhead Door - GE 2200A-L	55
Figure 26. Magnetic Contacts: Heavy Duty - Sentrol 2105.....	56
Figure 27. Push Button Exit Control - DynaLOCK 6270	57
Figure 28. BCD360V8-M-MP-C	57
Figure 29. Motion Detector - Bosch ISC-CDL1 & B328.....	58
Figure 30. DC Rack Mount ACS Power Supply - Altronix R615DC1016	60
Figure 31. Rackmount Server - BCDVideo BCD320E8-M-SAS-MP-C.....	61
Figure 32. Rackmount Server - BCD104-170-MP-C	62
Figure 33. Rack Mount DC Power Supply - AlarmSaf RM-PS5-MD-UL.....	63
Figure 34. Surface Mount Magnetic Contact - GE 2507A	65
Figure 35. Surface Mount Magnetic Contact - GE 2507AD	66
Figure 36. Digital Loop Protector - EPS 3416D	67
Figure 37. Digital Loop Protector - EPS 3416D	68
Figure 38. Pedestal - CEO 72-9C-D and LANDO-KY-20x14E	68
Figure 39. Pedestal - CEO 72-9C-D and LANDO-KY-20x14E	69
Figure 40. Honeywell FG-730	70
Figure 41. Exane Firewall LSZH Type TC	71
Figure 42. Synergis Architecture.....	76
Figure 43. Example of Access Denied Event.....	77
Figure 44. Security Center Access Control Integration.....	78
Figure 45. Genetec Synergis: About Config Tool: Version 5.7 SR3 (5.7.809.45)	80
Figure 46. Security Center: Architecture	81
Figure 47. Security Center Workstation Installation: Right-Click File and Select Properties.....	83

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 10 of 430

Figure 48. Security Center Workstation Installation: Unlock Security in General Tab.....	83
Figure 49. Security Center Workstation Installation: Select 'Extract All'	84
Figure 50. Security Center 5.x Client Installation: Setup.exe	84
Figure 51. Security Center 5.x Client Installation: NET Framework	84
Figure 52. Security Center 5.x Client Installer	85
Figure 53. Security Center 5.x Client Installation: Custom Setup.....	85
Figure 54. Security Center 5.x Client Installation: System Usage Participation	85
Figure 55. Genetec Security Desk – Hardware Benchmark Tool	86
Figure 56. Security Desk - Log On Window.....	87
Figure 57. Log On	88
Figure 58. Log on: Untrusted Directory	89
Figure 59. Log On: Invalid Certificate	89
Figure 60. Log On: Trusted Directory	89
Figure 61. Log On: Windows Credentials	90
Figure 62. Log On: Clear Windows Credentials: DOMAIN\Username	90
Figure 63. Passive Authentication Log On.....	91
Figure 64. Log On: Webform.....	92
Figure 65. Security Center 5.7 Basic Roles	93
Figure 66. Directory Role Disconnect: Video Cache	94
Figure 67. Directory Failure: Degraded Mode.....	95
Figure 68. System Architecture: Directory Role.....	95
Figure 69. System Architecture: Access Manager Role	96
Figure 70. Role Failover	99
Figure 71. Failover: Secondary Server	101
Figure 72. SQL Server Configuration Manager	103
Figure 73. Tile Displaying A Camera	108
Figure 74. Unpack Content in a Tile	111
Figure 75. Access Controller.....	112
Figure 76. Access Manager and its Doors	113
Figure 77. Access Manager and Access Logic.....	115
Figure 78. Access Control Rules: Access Control Task	116
Figure 79. Access Control Configuration: Area View: Access Rules.....	117
Figure 80. System Architecture: Access Rules.....	118
Figure 81. Access Rules: Scheduling	120
Figure 82. Access Rules: Deny Rule	126
Figure 83. Cardholder Management Task	127
Figure 84. Access Rights Overview	130
Figure 85. Image Editor.....	131
Figure 86. Picture Background: Chroma Color	132
Figure 87. Picture Background: Transparent	132
Figure 88. Automatic Entry.....	134
Figure 89. Encode OFF.....	134
Figure 90. Encode ON	134
Figure 91. Manual Entry	135
Figure 92. Cardholder Enter a PIN	135
Figure 93. Mobile Credential	136
Figure 94. Signature Pad	140
Figure 95. People Count	142
Figure 96. Cardholder Modification Dialog Box	146

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 11 of 430

Figure 97. Cardholder Groups	149
Figure 98. Event to Action.....	151
Figure 99. Credentials: Access Control Task.....	152
Figure 100. Credentials: Access Management Task	153
Figure 101. Credentials: Unused Credential & Cardholder Expiration	153
Figure 102. Credentials: Search Unused Credentials and Cardholders.....	154
Figure 103. Access Control Configuration: Credential Management	154
Figure 104. Cardholders and Credentials	155
Figure 105. Credential Management Task.....	156
Figure 106. Batch Enrollment: Automatic Credentials	158
Figure 107. Batch Enrollment: Manual Credentials	160
Figure 108. Create Credentials: Automatic Entry - Door	161
Figure 109. Create Credentials: Automatic Entry - Encode OFF.....	161
Figure 110. Create Credentials: Automatic Entry - Encode ON	162
Figure 111. Create Credentials: Manual Entry	162
Figure 112. Create Credentials: Manual Entry: PIN	162
Figure 113. Create Credentials: Manual Entry - Entity Name.....	163
Figure 114. View Area.....	170
Figure 115. Entity Cycling	171
Figure 116. Video Stream in Tile	171
Figure 117. Static Door Image	172
Figure 118. Door Entity	172
Figure 119. Door Widget.....	173
Figure 120. User Management: Config Tool.....	179
Figure 121. User Management: User Privileges	180
Figure 122. User Management: Unconfigured User	180
Figure 123. User Management: Remote Control	181
Figure 124. User Management: Resolving Conflicting Privileges.....	182
Figure 125. User Management: Users.....	182
Figure 126. Logon	187
Figure 127. User Management: Access Rights	188
Figure 128. Security Desk Properties	190
Figure 129. User Management: Config Tool - User Groups.....	192
Figure 130. User Management: Privileges.....	193
Figure 131. Privilege Exception	196
Figure 132. Privileges Exceptions.....	197
Figure 133. Access Control Configuration: Areas.....	201
Figure 134. Access Control Configuration: Area View.....	201
Figure 135. Areas: Area View	202
Figure 136. Area View.....	203
Figure 137. Schedule Management: Configuring a Schedule	207
Figure 138. Schedule Management: Specific Schedules	208
Figure 139. Access Control Configuration: Schedule Management	210
Figure 140. Schedule Management: Daily Schedule.....	214
Figure 141. Schedule Management: Weekly Schedule.....	215
Figure 142. Schedule Management: Ordinal Schedule	216
Figure 143. Schedule Management: Specific Dates.....	217
Figure 144. Schedule Management: Defining Twilight Schedules	218
Figure 145. Access Control Configuration: General Settings: Event Handling.....	223

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 12 of 430

Figure 146. Event Handling: Events to Actions	224
Figure 147. Event Handling: Security Center Actions.....	224
Figure 148. Event Handling: Event to Action	225
Figure 149. Event Handling: Event Colors.....	229
Figure 150. Access Control Configuration: General Settings: Configuring Event/Action	233
Figure 151. Access Control Configuration: General Settings: Zones	240
Figure 152. Access Control Configuration: Creating a Zone	241
Figure 153. Access Control Configuration: General Settings: In/Out Linking.....	242
Figure 154. Access Control Unit	244
Figure 155. Add Inputs to Zone	245
Figure 156. I/O Linking Example.....	246
Figure 157. Global I/O: Peer-to-Peer Communication on SCL.....	246
Figure 158. Global I/O; Peer to Peer Setup	247
Figure 159. Global I/O; Peer to Peer Configuration.....	248
Figure 160. I/O Zone Properties	249
Figure 161. Access Control Configuration: Roles: Import Cardholders from Active Directory	285
Figure 162. Benefits of Active Directory Integration	287
Figure 163. Synchronized Groups	293
Figure 164. Active Directory Attribute	295
Figure 165. Access Control Configuration: Areas: Antipassback and Interlocking.....	300
Figure 166. Interlock: Access Granted to 1 Door at a Time.....	304
Figure 167. Interlock: Interlock Override	305
Figure 168. Interlock: Lockdown	306
Figure 169. Access Control Configuration: General Settings: Add Custom Card Formats	308
Figure 170. Custom Card Format	308
Figure 171. Custom Card Format Editor	309
Figure 172. Importing Custom Card Formats	310
Figure 173. Custom Card Format Editor Tool.....	312
Figure 174. Access Control Configuration: General Settings: Custom Fields	315
Figure 175. Access Control Configuration: Global Cardholder Synchronization	316
Figure 176. Access Control Configuration: Badge Designer	318
Figure 177. Badge Template	319
Figure 178. Badge Template: Badge Designer.....	322
Figure 179. Badge Template: Display Barcode Properties.....	324
Figure 180. Badge Template: Dynamic/Static Images	325
Figure 181. Alarm Management: Active Alarm in Canvas Tile	327
Figure 182. Alarm Management: Alarm Acknowledgement Conditions	335
Figure 183. Alarm Management: Report an Incident.....	337
Figure 184. Alarm Management: Alarm Monitoring	338
Figure 185. Alarm Management: Alarm Options	338
Figure 186. Alarm Management: Popup Alarm Display.....	339
Figure 187. Alarm Management: Grouping Alarm	339
Figure 188. Alarm Filters.....	340
Figure 189. ICCS Generic Alarm Command.....	342
Figure 190. Alarm Management: Monitor Alarm Groups	343
Figure 191. Alarm Management: Trigger Alarm.....	344
Figure 192. Alarm Management: Event to Action	344
Figure 193. Alarm Management: Alarm Options	345
Figure 194. Alarm Management: Alarm Options	346

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 13 of 430

Figure 195. Alarm Management: Alarm Privileges	346
Figure 196. Genetec Security Desk – Alarm Report Task.....	348
Figure 197. Alarm Management: Alarm Report	349
Figure 198. Event/Alarm Flows	351
Figure 199. Alarm Management: Operational Alarms	352
Figure 200. Alarm Management: Genetec Alarms	353
Figure 201. Security Desk – Area Activities Task.....	355
Figure 202. Reports: Line Charts: Cardholder Event Report.....	357
Figure 203. Reports: Simplified Line Chart.....	357
Figure 204. Reports: Column Chart: Door Access Report.....	358
Figure 205. Reports: Stacked Columns: Door Activities Report.....	358
Figure 206. Reports Rows: Intrusion detector report.....	359
Figure 207. Reports: Stacked Rows: Intrusion Detector Report.....	359
Figure 208. Pie Chart: Camera Events and Motion Report	360
Figure 209. Doughnut Chart: Camera Events and Motion Report.....	360
Figure 210. Reports: Reason Required Dialog	361
Figure 211. Reports: Chart Type Dropdown Menu	364
Figure 212. Reports: Donut Chart: Top 10 Camera Events.....	364
Figure 213. Reports: Line Chart: Top 5 Cardholder Events	365
Figure 214. Security Center Tools	368
Figure 215. Security Center Tools: Unit Replacement Tool	372
Figure 216. Security Center Tools: Unit Replacement	373
Figure 217. Security Center Tools: Move Unit Tool.....	374
Figure 218. Security Center Tools: Copy Config Tool	375
Figure 219. Upgrade Firmware	379
Figure 220. Upgrade Firmware	381
Figure 221. Upgrade Firmware: Delay Upgrade.....	381
Figure 222. Scheduled Tasks: Properties: Schedule Routine Reports	385
Figure 223. Security Center Troubleshooting – Hardware Inventory Report.....	386
Figure 224. Genetec Security Desk – View System Messages.....	390

List of Tables

Table 1. Specifications - BCDVideo BCD230T CPU 30
Table 2. Badge Printer (Sublimation/Thermal) - HID Fargo HDP5000 31
Table 3. ID Badge Camera - SoftwareHouse 20K758USB-SYS 35
Table 4. Signature Pad - Topaz Systems SigLit 36
Table 5. HP LaserJet Enterprise 700 M712xh Printer 38
Table 6. Access Card - HID 1386-LGGMN ISOProx II 42
Table 7. SmartCard Reader - HID 920P MultiClass SE Readers 42
Table 8. In/Out Module - Genetec Mercury Security MR-16IN I/O Module 45
Table 9. In/Out Module - Genetec Mercury Security MR-16OUT Module 46
Table 10. In/Out Module - Genetec Mercury Security MR-16OUT Module 47
Table 11. Telephone Entry - Ameristar Gate 1837AGS 49
Table 12. Request to Exit Detector and TP160 Trim Plates - Bosch DS150i 51
Table 13. GE Interlogix 1078 Series Steel Door Contacts 53

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 14 of 430

Table 14. Industrial Surface Mount Contact - Sentrol 1045 Position Sensors	53
Table 15. Key Switch - Camden CM1170-7024	55
Table 16. Magnetic Contacts: Overhead Door - GE 2200A-L	55
Table 17. Magnetic Contacts: Heavy Duty - Sentrol 2105: Specifications	56
Table 18. Push Button Exit Control - DynaLOCK 6270: Specifications	57
Table 19. BCD360V8-M-MP-C: Specifications	58
Table 20. Motion Detector - Bosch ISC-CDL1 & B328: Specifications	59
Table 21. DC Rack Mount ACS Power Supply - Altronix R615DC1016	60
Table 22. Rackmount Server - BCDVideo BCD320E8-M-SAS-MP-C	61
Table 23. Rackmount Server - BCD104-170-MP-C	62
Table 24. Rack Mount DC Power Supply - AlarmSaf RM-PS5-MD-UL	63
Table 25. Surface Mount Magnetic Contact - GE 2507A	65
Table 26. Surface Mount Magnetic Contact - GE 2507AD	66
Table 27. Digital Loop Protector EPS 3416D Specifications	68
Table 28. Pedestal - CEO 72-9C-D and LANDO-KY-20x14E	69
Table 29. Honeywell FG-730 Glass Break Detector Features	70
Table 30. Exane Firewall KSZH Type TC Specifications	71
Table 31. Security Center Roles that Support Failover	99
Table 32. Access Control Entities	107
Table 33. Tile Menu Commands	109
Table 34. Event-to-Action Conditions	236
Table 35. Event-to-Action Identifiers	237
Table 36. Types of Zones	250
Table 37. Event Acknowledgement Conditions	334
Table 38. Alarm Management: Clear Source Condition	337
Table 39. Security Center Tools: Copy Configuration Tool: Entities Setting Categories	376
Table 40. Genetec Security Desk – Types of Reports Available	382

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 15 of 430

1 SCOPE

The Honolulu Authority for Rapid Transportation (HART) is building America's first fully-automated driverless, urban light metro rail system. This light rail system is the first for the State of Hawaii and will link key employment centers, and residential communities along a 20-mile corridor with 21 stations along the south shore of the Hawaiian island of Oahu. The scope of this document provides operations information on the Communications System (COMMS) in support of HART operations.

1.1 PURPOSE

This document describes how to use the Genetec Synergis application for access control within the Integrated Communications Control System (ICCS). It provides a comprehensive overview of the HART Access Control System (ACS), how to operate the Genetec Synergis application for onboarding staff to this program as they are used in the Network Operations Center (NOC) and the Operations Control Center (OCC). [Figure 1](#) illustrates how the ICCS software components are divided across five HART manuals.

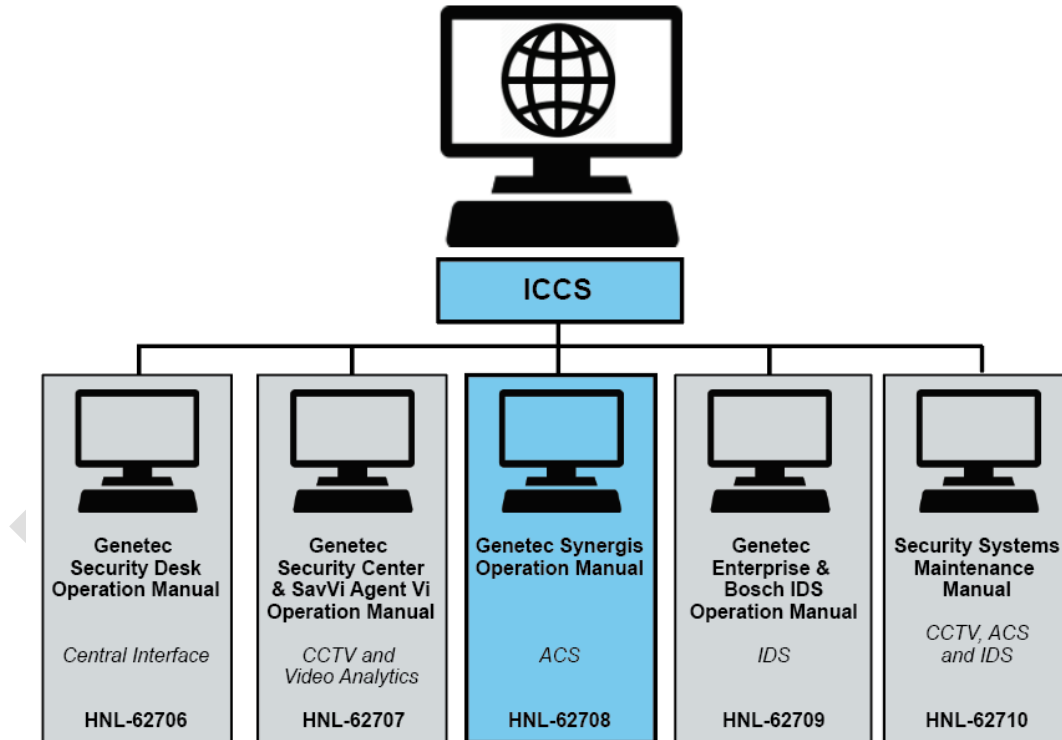


Figure 1. Organization of HART ICCS Security System by Manual

1.2 APPLICABILITY

This document applies to the HRH Core Systems Contract (CSC), which involves Design-Build (DB) phases of the Core Systems for Honolulu Rail Transit Project (H RTP).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 16 of 430

1.3 REFERENCE DOCUMENTS

The latest versions of the reference documents listed below and available on the Ansaldo Signaling and Transportation Systems (ASTS) intranet (in Teamcenter for H RTP under Project Code 0182T, or at the SharePoint site titled “Honolulu”), shall be followed, except where a specific revision number of a reference document is indicated.

1.3.1 Contractual Reference Documents

The following contractual documents were used as reference material in this document.

- A. General Provisions
- B. Special Provisions
 - 1. SP Section 4.7.e.2.C
- C. Technical Provisions Document 3 (TP-3)
 - 1. Section 3.2.4 – Operating Manuals
 - 2. Section 3.2.5 – Maintenance Manuals
 - 3. Section 3.2.7 – Training Plan and Program
 - 4. Section 3.5.2.7 – Maintenance Tools and Equipment
- D. Technical Provisions Document 4 (TP-4)
 - 1. TP-4.7.4.12 – System Maps and Display Panels
 - 2. TP-4.7.20 – Video Monitoring and Communications Systems
- E. Technical Provisions Document 7 (TP-7)
 - 1. Section 28 13 00 – Access Control System
 - 2. Section 28 16 00 – Intrusion Detection
- F. Technical Provisions Document 9 (TP-9)
 - 1. Section 9 21.0 – Fire and Intrusion Alarm Systems
- G. Technical Provisions Document Management Provisions (MP-02)
 - 1. Section 2.14 – Security Admin Activities
- H. Section 2.4 – Training of Operations and Maintenance (O&M) Personnel

1.3.2 Project Reference Documents

The following project documents were used as reference material in this document.

- 1. HNL-02000 Quality Assurance Plan
- 2. HNL-02001 Document Format
- 3. HNL-02002 Quality Implementing Procedure – Document Coding
- 4. HNL-02004 Quality Implementing Procedure – CADD Standardization
- 5. HNL-09012 Guidelines for O&M Manuals
- 6. HNL-09014 Preliminary Training Description
- 7. HNL-21001 Communications System Purchase Technical Specification
- 8. HNL-40003 Communications System – Supportive Quality Plan
- 9. HNL-60112 Communications System – IDS Technical Specification
- 10. HNL-60113 Communications System – ACS Technical Specification
- 11. HNL-60630 Communications System – ICCS Product Configuration Framework

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 17 of 430

12. HNL-60308 Communications System – ICCS Technical Specification
13. HNL-60125 Communications System – IDS Data Sheet
14. HNL-61744 Communications System – Training and O&M Materials Plan

1.3.3 International, National, and Local Reference Standards

The following is a representative list of codes and standards for the communications system. HRH will comply with all applicable codes, standards, and other requirements as required by the contract. The governing version of the listed documents shall be the latest as adopted and administered or approved by the City. In the event any reference or standard cited herein is superseded by another reference or standard, the latest version in effect on the date of the Request for Proposals shall be used.

- A. Electromagnetic Compatibility (EMC)
 1. EMC Emission – EN55022 Class A
 2. EMC Immunity – EN50082-1
- B. Federal Communications Commission (FCC)
 1. FCC Title 47 CFR Part 15 Subpart B Class B
- C. Institute of Electrical and Electronics Engineers (IEEE)
 1. 802.1p Traffic Priority and Dynamic Multicast Filtering In LANS
 2. IEEE 802.1ag Service Layer Operations, Administration and Maintenance (OAM) (Connectivity Fault Management)
 3. 802.1Q VLAN standard
 4. 802.3 Ethernet LAN
 5. 802.3u Network Maintenance
 6. 802.3ab Gigabit Ethernet Over Twisted Pair Cabling 1000Base-T
 7. IEEE 1613 Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations
 8. IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
- D. International Electro Technical Institute (IEC)
 1. IEC 61000 Electromagnetic Compatibility (EMC)
 2. IEC 60529 Ingress Protection (IP)
- E. Metro Ethernet Forum (MEF)
 1. MEF-9 Metro Ethernet Forum Product Certification
 2. MEF-14 Metro Ethernet Network Architecture
- F. Simple Network Management Protocol (SNMP)
 1. SNMPv1 and v2 Network Management Protocols
 2. SNMPv3 Authentication & Encryption for Security
- G. European Committee for Electrotechnical Standardization (CENELEC)
 1. EN 50155:2007 Railway Applications – Electronic equipment used on rolling stock

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 18 of 430

1.4 TERMS, ACRONYMS, AND ABBREVIATIONS

Acronym	Definition
2D	Two Dimensional
AA	Advanced Authorization (former process; replaced by OLA/OXIA/RSM)
ACS	Access Control System
AED	Automated External Defibrillator
AG	At Grade
ALU	Alcatel-Lucent
ANI	Automatic Number Identification
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ASTS	Ansaldo Signaling and Transportation Systems
ATEL	Administrative Telephone
BLS	Blue Light Station
BOCC	Backup Operation Control Centre
BOM	Bill of Materials
CADD	Computer-Aided Drafting Drawing
CCB	Change Control Board
CCH	City and County of Honolulu
CCTV	Closed Circuit Television
CENELEC	European Committee for Electrotechnical Standardization
CFR	Code of Federal Regulations
CIC	Communications Interface Cabinet
CIF	Common Intermediate Format
CIP	Contract Implementation Process
City	The City and County of Honolulu
COMMS	Communication System
CPU	Central Processing Unit
CQAP	Contractor's Quality Assurance Program
CSC	Core Systems Contract
CTS	Communication Transmission System
DB	Design Build
dBA	Decibels, A weighted
DBU	Database Unit
DD	Definitive Design
DMS	Document Management System
DMT	Degraded Mode Terminal
DOA	Dead On Arrival
DOC	Declaration of Conformity

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 19 of 430

Acronym	Definition
EMC	Electromagnetic Compatibility
EMEA	Europe, Middle East, Africa
EMI	Electromagnetic Interference
ESD	Electronic Static Discharge
ETEL	Emergency Telephone
EXIF	Exchangeable Image File
FACP	Fire Alarm Control Panel
FCC	Federal Communications Commission
FD	Final Design
FTEL	Fire Telephone
GUI	Graphical User Interface
HART	Honolulu Authority for Rapid Transportation
HRH	Hitachi Rail Honolulu (Joint Venture)
HRIT	Hitachi Rail S.p.A
H RTP	Honolulu Rail Transit Project
Hz	Hertz
I/O	Input / Output
IAAP	Intrusion Alarm Annunciator Panel
IC	Intercom System
ICCS	Integrated Control Center Software
ICMS	Integrated Communications Management System
IDS	Intrusion Detection System
IEC	International Electro Technical Institute
IEEE	Institute of Electrical and Electronics Engineers
INMS	Integrated Network Management System
IR	Infrared
ITU-T	International Telecommunication Union Standardization
LAN	Local Area Network
LCD	Lean Customer Delivery
LCD	Liquid Crystal Display
LED	Light Emitted Diode Technology
LRU	Lowest Replaceable Unit
MEF	Metro Ethernet Forum
MMIS	Maintenance Management Information System
MP	Management Provisions
MSF	Maintenance and Storage Facility
NEC	National Electrical Code
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Association

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 20 of 430

Acronym	Definition
NOC	Network Operations Center
O&M	Operations and Maintenance
OAM	Operations, Administration and Maintenance
OBS	On-Board System
OCC	Operations Control Center
PA	Public Announcement
PABX	Private Automatic Branch Exchange
PIS	Passenger Information System
PM	Project Management
PO	Purchase Order
POE	Power Over Ethernet
PS	Power Supply
PTZ	Pan Tilt Zoom
QA	Quality Assurance
QA&CC	Quality Assurance & Customer Care
QIP	Quality Improvement Program
QMS	Quality Management System
RAID	Redundant Array of Independent Disks
RFM	Ready for Maintenance (CIP Milestone)
RFP	Request for Proposal
RTM	Requirement Traceability Matrix
SAN	Storage Area Network
SCADA	Supervisory Control and Data Acquisition
SDK	Software Development Kit
SLAN	Station Local Area Network
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
STS	Hitachi Rail STS
TCCR	Train Control Communications Room
TCP/IP	Transmission Control Protocol/Internet Protocol
TEL	Telephone System
TP	Technical Provision
TPSS/GBS	Traction Power Substation/Gap-Breaker Station
TR	Test Report
TS	Telephone System
UL	Underwriters Laboratories, Inc.
UTC	Universal Time Coordinated
Vac	Volts, alternating current
Vdc	Volts, direct current

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 21 of 430

1.5 DESCRIPTION OF CHANGES

Not applicable as this is the first issue.

1.6 DOCUMENT ORGANIZATION

This manual is organized in the same structure as other HART operation and maintenance manuals.

1.6.1 HART ACS Operations Manual Organization

Figure 2. ACS Operations Manual Organization is a graphic representation of how this manual is organized.

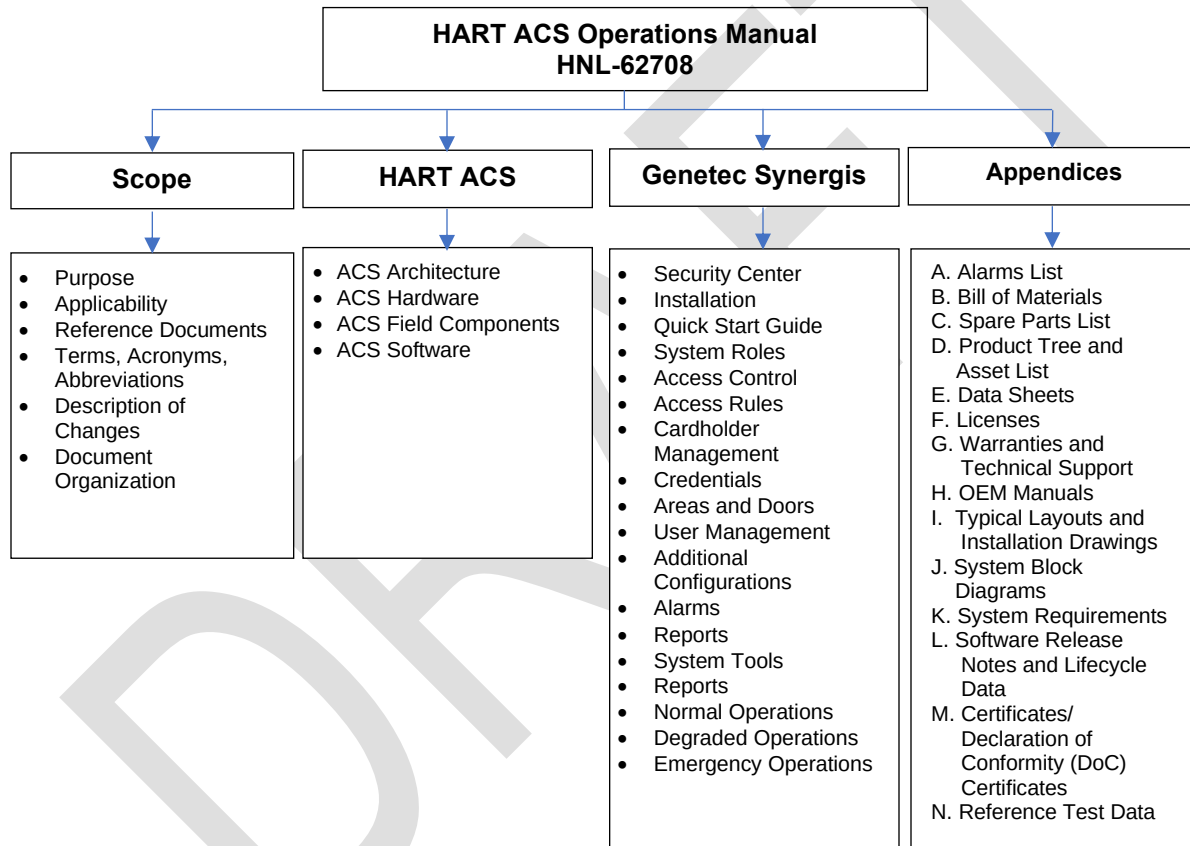


Figure 2. ACS Operations Manual Organization

1.6.2 HART Communications System Operations and Maintenance Manuals

The HART Communications System includes the following operations and maintenance manuals.

1. HNL-62700 Network Operations and Maintenance Manual
2. HNL-62701 Network Timing System (NTS) Operations and Maintenance Manual

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 22 of 430

3. HNL-62702 Integrated Network Management System (INMS) Operations and Maintenance Manual
4. HNL-62703 Wireless Communication System (WCS) Operations and Maintenance Manual
5. HNL-62704 Maintenance Management Information System (MMIS) Operations Manual
6. HNL-62705 Maintenance Management Information System (MMIS) Maintenance Manual
7. HNL-62706 Integrated Communications Control System (ICCS) Operations Manual
8. HNL-62707 Security System: Closed Circuit Television (CCTV) Operations Manual
9. HNL-62708 Security System: Access Control System (ACS) Operations Manual (this document)
10. HNL-62709 Security System: Intrusion Detection System (IDS) Operations Manual
11. HNL-62710 Security System Maintenance Manual
12. HNL-62711 Passenger Information System (PIS) Public Address (PA) Operations Manual
13. HNL-62712 Passenger Information System (PIS) Variable Message Sign (VMS) Operations Manual
14. HNL-62713 Passenger Information System (PIS) Maintenance Manual
15. HNL-62714 Telephone System (TS) Operations Manual
16. HNL-62715 Telephone System (TS) Maintenance Manual
17. HNL-62716 On Board System (OBS) Operations Manual
18. HNL-62717 On Board System (OBS) Maintenance Manual

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 23 of 430

2 HART ACS

The HART Access Control System (ACS) and Intrusion Detection System (IDS) are an integrated suite of software and hardware devices. The ACS ensures that only authorized persons enter certain areas and facilities. These include enclosures at TPSSs and GBSSs, the pedestrian entrance at the main MSF gate; and the internal gate to access the MSF secondary access roadway. Within the MSF, the visitors' gate is access-controlled to ensure that only escorted visitors enter employee-only areas. Access to the storeroom is also limited to authorized persons, as is access to the OCC.

During normal revenue operations, the ACS allows open access to all public areas through all designated public entrances. During non-revenue operation hours, the access to non-public and public areas is limited to authorized persons with card keys. Provisions are made for authorized persons at certain locations inside the building to activate the release of certain restricted-access doors following voice communication from the door to the operator inside. Provisions are also made for emergency access by the fire department, police, or emergency medical personnel by keyed switch or other method to all areas via all entrances, including station and maintenance facilities emergency exits using a Knox Box system.

The ACS at the OCC protects all the vital and commercial central computers, equipment rooms housing the train control and communications equipment, OCC system computers/servers and communications equipment, the associated engineering management/maintenance terminals, and support facilities.

The ACS is integrated with the CCTV system to provide event-driven video of events and alarms at all stations and facilities within the system. Using a central server, the ACS, IDS, and CCTV systems provide integrated event information and video to the integration software in the OCC.

Main equipment located at the OCC include:

- Administrator's Workstation – mouse-driven
- 24-inch flat-panel monitor
- System printer
- Badge printer
- Signature pad
- Flex-camera for photograph ID
- Signature pad

The system is equipped with card keys and all accessories to properly create and manage users.

2.1 ACS ARCHITECTURE

The ACS/IDS is based on a distributed architecture and consists of a central management system and field panels with attached signal imitation and control devices throughout the Honolulu Light Rail stations and Maintenance and Storage Facility (MSF) locations.

The ACS controls restricted areas via a preauthorized credential that alerts the security operators to unauthorized access attempts, door violations, and other system events that it interfaces with. The access control and management system support configuration changes, reader control, and displays current conditions, system troubles and alarms over a TCP/IP connection. It is responsible for executing commands and monitoring the overall ACS.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 24 of 430

The ACS communicates via the Communication Transmission System (CTS) and Station Local Area Network (SLAN); ACS panels are distributed in station Train Control Communications Room (TCCR), MSF equipment rooms, Traction Power Substation/Gap-Breaker Station (TPSS/GBS) locations, and other technical rooms where required. These panels are connected to the SLAN all communicating back to a centralized server via the CTS network. [Figure 3](#) depicts the HART ACS/IDS architecture.

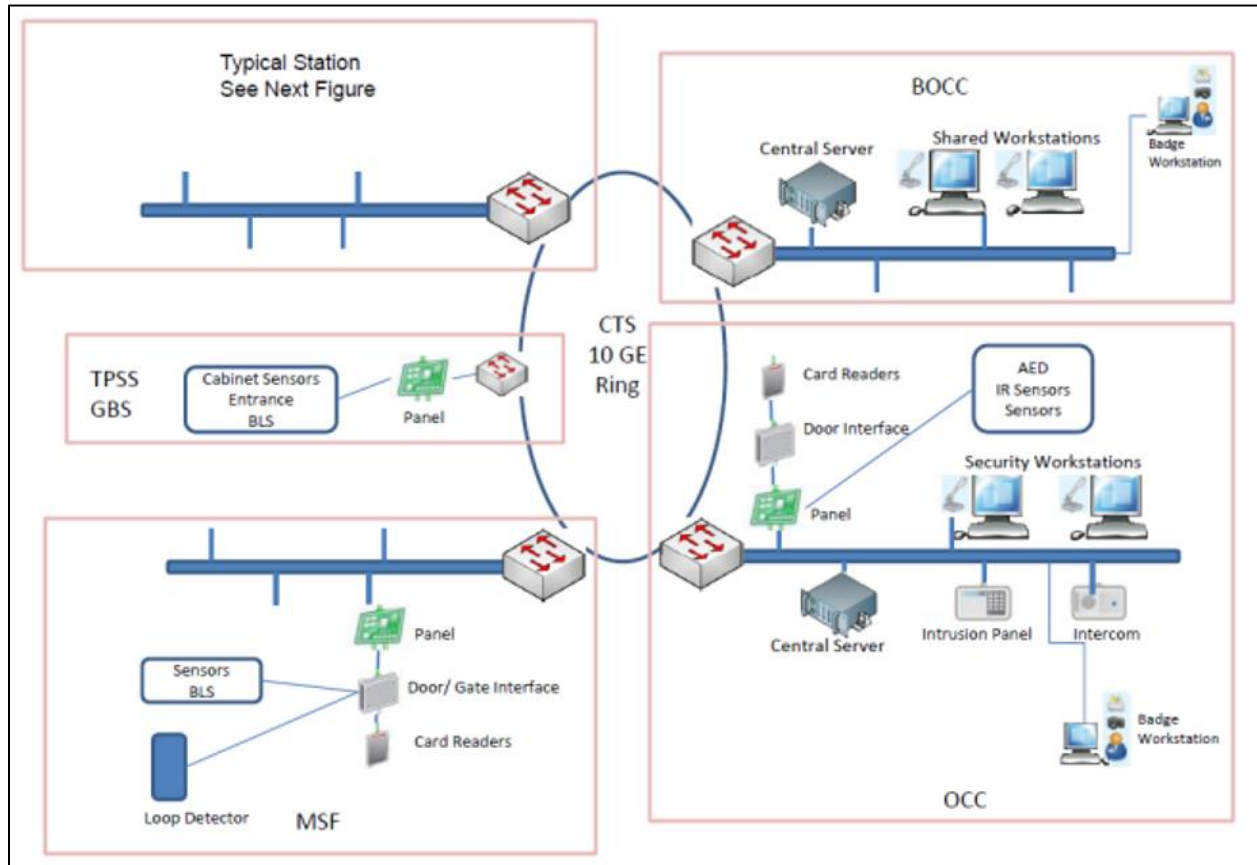


Figure 3. HART ACS/IDS Architecture

As part of the ACS, the IDS uses the same distributed field panels, alarm initiation devices, and control keypads thought the system. It monitors system devices and locations for after-hours intrusion and alerts the security operator to the event location. The IDS monitors intrusions to specific areas on a 24-hour basis, such as end-of-platform gates and other restricted areas.

Multiple functional and geographic zones automatically provide different levels of monitoring and access control to different parts of the system. Like the ACS, IDS also communicates via the CTS and SLAN networks - intrusion detection panels are also distributed in station TCCR and MSF equipment rooms and connect to the SLAN, which all report back to a central server via the CTS.

Both systems are integrated with the CCTV system to provide event video of events and alarms at all stations and facilities within the HART system. Using a central server, the ACS, IDS, and CCTV systems provide integrated event information and video to security personnel in the OCC

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 25 of 430

Figure 4 provides a view of the station layout. Access control devices for a typical station include card readers, an interface, and an access control panel. Depending on how the panel is configured, it can send alerts for an automated external defibrillator (AED), Blue Light Station (BLS) telephones, Infrared (IR) sensors, or door sensors. Access control devices for TCCR include an intrusion panel and control panel configured for cabinet sensors, TCCR door, or an electric room door. The communication is transmitted along a SLAN to an access-controlled door, whether it's a one-way or two-way door.

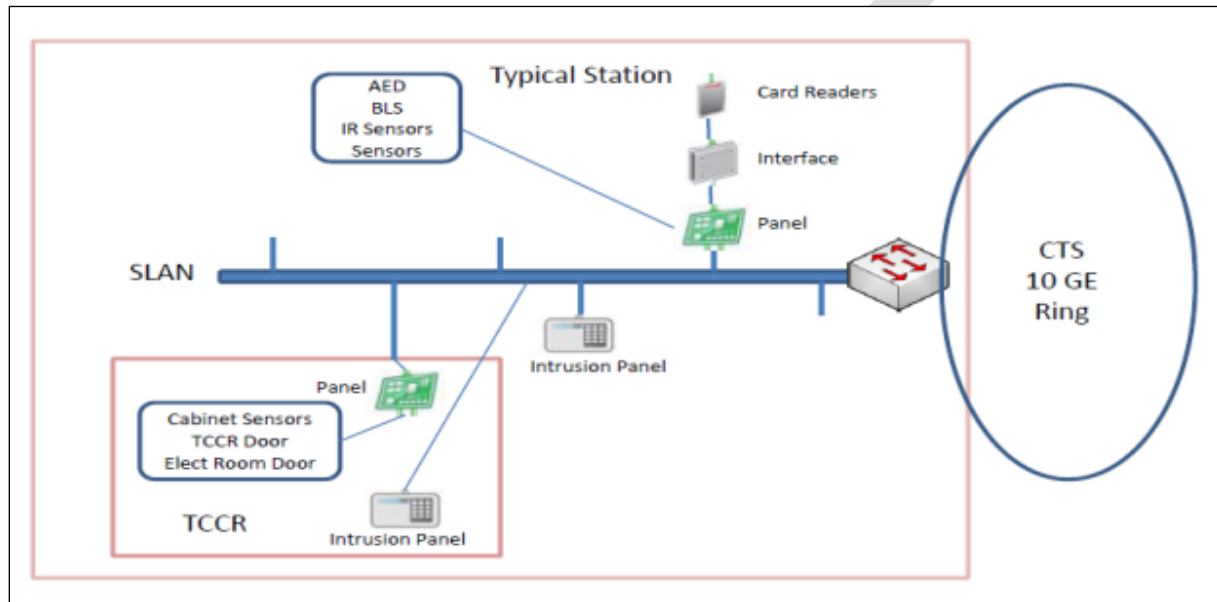


Figure 4. ACS: Typical Station Layout

Figure 5 shows the OCC has the following hardware architecture.

- Badge workstation with a signature pad
- Alarm workstation with the printer to print hard copy reports
- Application server
- Domain controller
- Primary directory server
- Primary plan manager server
- Two primary integrated manager servers
- Three active access manager cluster servers

The BOCC has architecture has a similar, yet not the same architecture as the OCC:

- Badge workstation with a signature pad
- Alarm workstation with the printer to print hard copy reports
- Storage Area Network (SAN) (Witness Server)
- Domain controller
- Failover directory server

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 26 of 430

- Failover plan manager server
- Two failover integrated manager server
- Three failover Access Manager cluster servers

The MSF, Yard facilities, and TPSS all connect to the LAN/WAN via IACP. The MSF Yard entrance/guardhouse uses an intercom that connects to the LAN/WAN.

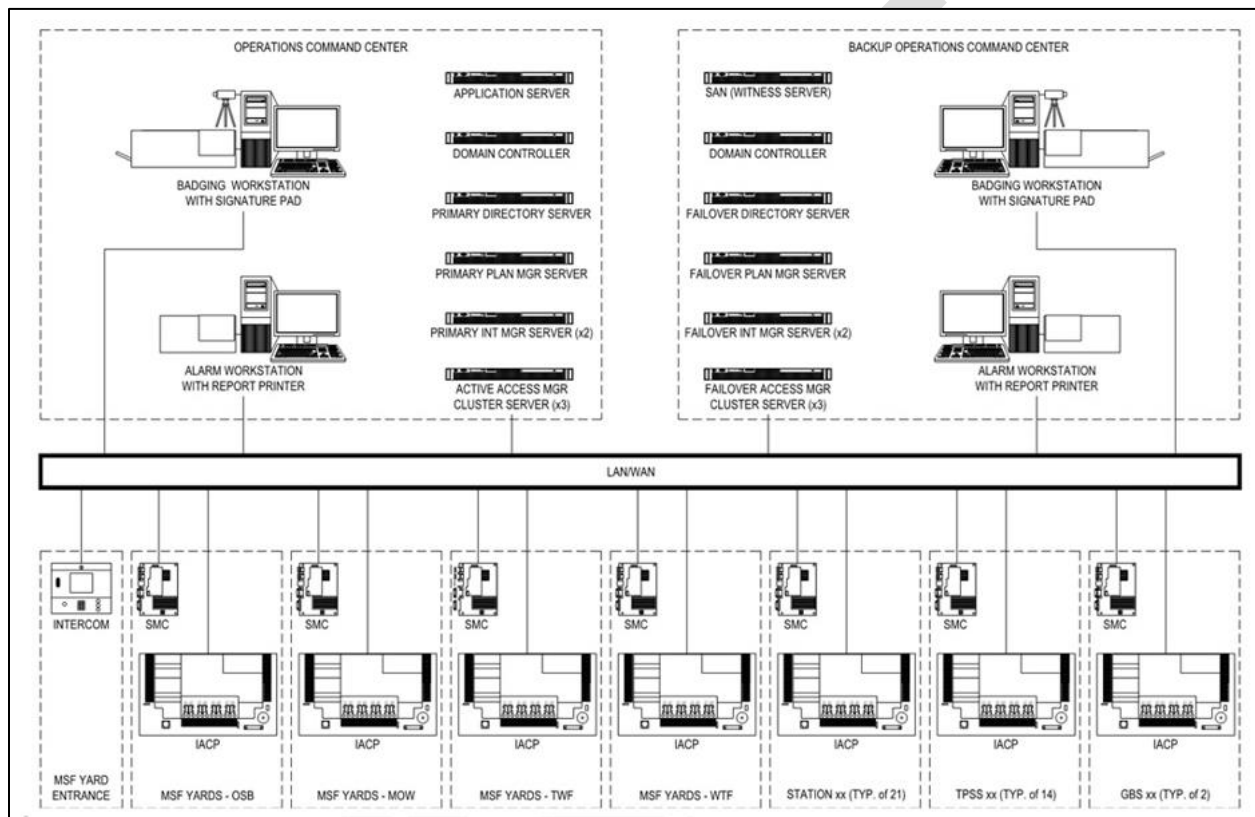


Figure 5. ACS/IDS Architecture for OCC, BOCC, MS , TPSS and GBS

If the main system fails or is out of service due to a CPU failure, its functions will transfer to the backup system through the failover services process, ensuring the continuity of the operations.

Figure 6 shows the typical architecture of ACS/IDS inside a station or building. On the left side of the figure, a door, louver, glass break detector, communication system cabinet, or tamper software connect to an Access Control Panel (ACP). The ACP connects to an SMC power supply unit, a power supply, and an AC power supply unit. The SMC and ACP connect to the LAN/WAN. The IACP triggers the bell or Knox Box.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 27 of 430

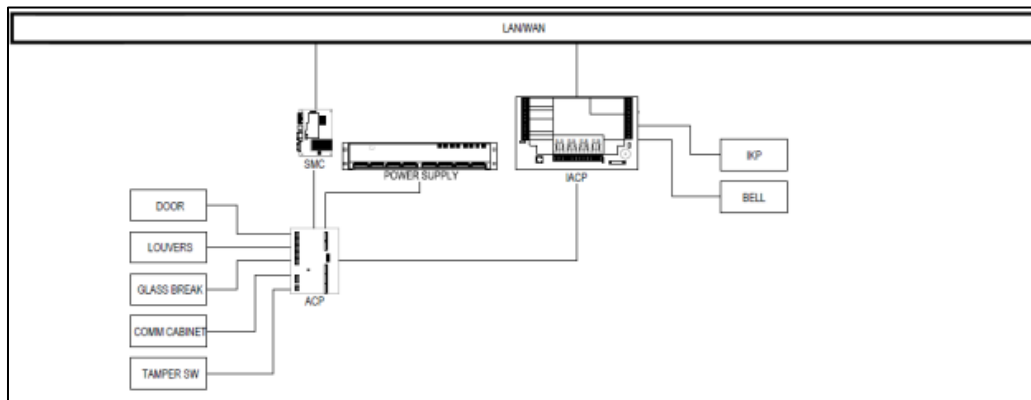


Figure 6. ACS/IDS Architecture for Stations or Buildings

Figure 7 shows the deployment of various ACS/IDS devices and how they connect to the network.

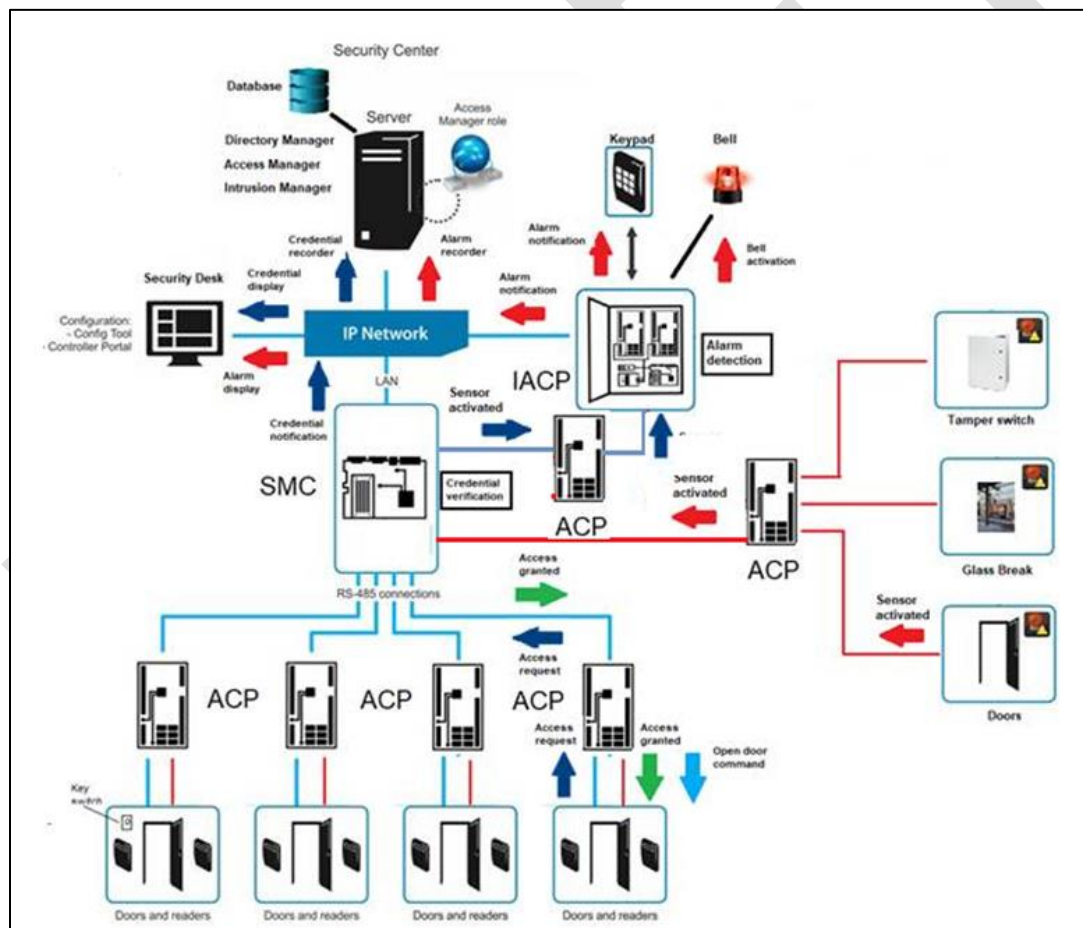


Figure 7. ACS/IDS Device Deployment

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 28 of 430

2.1.1 Servers

The ACS/IDS consists of a flexible, open architecture and operates on most reliable platforms, including Windows Operating System and utilizes MS SQL and Oracle server databases and storage platforms. The ACS server uses a single database and a single user interface for all ACS/IDS applications, including alarm control and credential management, etc.

Two ACS/IDS servers are deployed in the network in a 'hot-standby' mode. One is located in the OCC and the second in the BOCC. Should one server fail or lose communications with the network, the other is designed to continue operations without interruption.

The ACS/IDS server minimum hardware requirements are:

- CPU: Intel Xeon E5620 Quad-Core, 2.4GHz, 12MB L3 Cache
- Operating System: Windows Server 2008 R2 Standard SP1
- RAM: 4GB (2 x 2GB) 1333MHz dual-ranked UDIMMs
- Backplane: 1x8 Backplane for 2.5-inch Hard Drives
- RAID Controller: SAS 6/iR Integrated
- Disk Drives: 160 GB 7.2K RPM SATA 3Gbps 2.5-inch Hot Plug Hard Drives
- Power: 120/220V 570Watt Redundant Power Supply

2.1.1.1 Directory Server

Directory Server is the host servers of the Access Control Systems. The Directory role identifies a Security Center system. It manages all entity configurations and system-wide settings. Only a single instance of this role is permitted on your system. The server hosting the **Directory role** is called the main server and must be set up first. All other servers you add in Security Center are called expansion servers and must connect to the main server to be part of the same system.

2.1.1.2 Domain Controller

A domain controller (DC) is a server computer that responds to security authentication requests within a computer domain. It is a server on a network that is responsible for allowing host access to domain resources. It authenticates users, stores user account information, and enforces security policy for a domain. It is most commonly implemented in Windows environments, where it is the centerpiece of the Windows Active Directory service. The Domain Controller manages the ACS Windows Domain.

2.1.2 Workstations

The security workstations used in the CCTV system are the same workstations used for the ACS/IDS. The ACS/IDS interface is a thin client, browser-based interface that allows direct connection to the ACS/IDS server. This interface allows the operator to respond to alarms, configure hardware, and review system logs. The operator can also review and clear alarms from intrusion detection panels remotely. Two security workstations are located in the OCC and support the CCTV system with three monitors each.

All operator workstations in the OCC and BOCC are capable of viewing and manipulating images through the ICCS. The ICCS provides the primary interface for the operators and uses an API to the CCTV video management server.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 29 of 430

2.1.2.1 Badge Workstation

A badge workstation lets authorized personnel create user access credentials. The badge workstation is connected to the ACS/IDS servers through the OCC LAN and CTS. It consists of:

- Desktop workstation
- Badge printer/encoder
- IP camera
- Credential software
- Background screen

The badge workstation is the primary interface to the enrollment of all credentials and their associated personnel.

2.1.2.2 CPU Tower – BCD Video BCD230T

The BCD Video's Gamma Series CPU is designed specifically for commercial environments such as Access Control and IP video surveillance. The solution is designed to run in 24/7/365 applications and powerful enough to render high-quality megapixel images.



Figure 8. BCDVideo BCD230T

[Table 1](#) provides a list of specifications for the CPU.

Table 1. Specifications - BCDVideo BCD230T CPU

Specification		Description	
Processor	(1) Intel E3 Xeon Processor	Form Factor	Tower
Processor Passmark	E3-1225V3—6832 E3-1245V3—9538 E3-1270V3—10171	Dimensions (W x H x D)	6.7 x 15.7 x 17.4 in
Operating System	Windows 7 Pro—64 bit	Hard Drives	500GB

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 30 of 430

Specification		Description	
Monitor Output-Embedded Graphics	(2) Display Port & (1) DVI	Power Supply	400 Watt
Optional Graphics Card Slot	(2) PCIe x16 - Low Profile	Warranty	Lifetime Phone Support 3-Year Global NBD Onsite

Refer to Appendix E: Datasheets, “HNL-60126 06.00-21- 4C047 BCDVideo BCD230T.pdf.”

2.1.2.3 Badge Printer (Sublimation/Thermal) - HID Fargo HDP5000

The HID Fargo sublimation badge printer provides superior print quality, higher reliability, and durability, greater security, so photo ID cards have all these qualities when you print and encode them. This card printer/encoder has a versatile modular design, dual card input hopper, dual-sided printing, single- or dual-sided lamination, and card encoding technologies. Minimal training is required because of its simple design and intuitive operation. Cards, ribbons, and overlaminates come in cartridges that load quickly and easily.



Figure 9. BCDVideo BCD230T Badge Printer

[Table 2](#) provides a list of specifications for the badge printer.

Table 2. Badge Printer (Sublimation/Thermal) - HID Fargo HDP5000

Specifications	Description
Print Method	HDP Dye-Sublimation / Resin Thermal Transfer.
Resolution	300 dpi (11.8 dots/mm).
Colors	Up to 16.7 million / 256 shades per pixel.
Print Ribbon Options	Full color, YMC*, 750 prints. Full color with resin black, YMCK*, 500 prints. Full color with two resin black panels, YMCKK*, 500 prints. Full color with resin black and heat seal panel for difficult-to-print surfaces, YMCKH*, 500 prints.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 31 of 430

Specifications	Description
	Full color with resin black and inhibit panel for signature or other non-printing areas, YMCKI*, 500 prints. Full color with fluorescing and resin black, YMCFFK*, 500 prints. Resin black, K, 3000 prints.
HDP Film Options	Clear (1,500 prints) • Standard Holographic (500 prints). Custom Holographic, special order (500 prints).
Overlamine Options	Thermal Transfer Overlamine, .25 mil thick, 500 prints. PolyGuard® Overlamine, 1.0 mil, and .6 mil thick, 250 prints (PolyGuard available in a CR-80 patch size). All overlaminates available in clear, standard holographic design or custom holographic design
Print Speed**	Batch Mode: 26 seconds per card / 138 cards per hour (YMC with transfer) *. 32 seconds per card / 113 cards per hour (YMCK with transfer) *. 47 seconds per card / 77 cards per hour (YMCKK with transfer) *. 37 seconds per card / 97 cards per hour (YMCK with transfer and dual-sided, simultaneous lamination) *. 55 seconds per card / 65 cards per hour (YMCKK with transfer and dual-sided, simultaneous lamination) *.
Accepted Standard Card Sizes	CR-80 (3.370" L x 2.125" W / 85.6mmL x 54mmW).
Print Area	Over-the-edge on CR-80 cards.
Accepted Card Thickness	Print only: .030" (30 mil) to .050" (50 mil) / .762mm to 1.27mm. Print/Lamination: .030" (30 mil) to .050" (50 mil) / .762mm to 1.27mm.
Accepted Card Types	ABS, Laminated PVC, PET, PETG, proximity, smart and mag stripe cards, optical memory cards. Note: ABS and PVC cards are not recommended for use in the HDP5000 Lamination Module***.
Input Card Cartridge Capacity	100 cards (.030" / .762mm).
Output Hopper Card Capacity	200 cards (.030" / .762mm).
Card Cleaning	Replaceable cleaning roller (included with each print ribbon).
Memory	16MB RAM.
Display	User-friendly, SmartScreen™ LCD Control Panel.
Software Drivers	Windows® 2000 / XP / Server 2003 / Vista (32 & 64 bit) / 7 (32 & 64 bit); Mac OS X v10.4 / v10.5; and Linux****.
Single Wire USB 2.0 Encoding Options	ISO Magnetic Stripe Encoding, dual high- and low-coercivity, Tracks 1, 2, and 3. Contactless Smart Card Encoder (HID iCLASS and MIFARE).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 32 of 430

Specifications	Description
	Contact Smart Card Encoder reads from and writes to all ISO7816-1/2/3/4 memory and microprocessor smart cards (T=0, T=1) as well as synchronous cards. Prox Card Reader (HID read-only) • iCLASS® Programming Platform Kit.
Interface	USB 2.0 (high speed) and Ethernet with internal print server.
System Requirements	x86 based PC or compatible, Windows 2000, Windows XP, Windows 2003, or Windows Vista, 500MHz computer with 256MB of RAM or higher, 500MB free hard disk space or higher.
Operating Temperature	65° to 90° F / 18° to 32° C.
Supply Voltage	100-240 VAC, 3.3 A.
Humidity	20 - 80% non-condensing.
Dimensions	HDP5000: 11.50" H x 12.25" W x 9.25" D / 292mmH x 313mmW x 235mmD. HDP5000 + Dual-Sided Module: 11.50" H x 17.50" W x 9.25" D / 292mmH x 445mmW x 235mmD. HDP5000 + Single-Sided Lam Module: 12.75" H x 25" W x 9.25" D / 324mmH x 635mmW x 235mmD. HDP5000 + Dual-Sided Module + Dual-Sided Lam Module: 12.75" H x 30" W x 9.25" D / 324mmH x 762mmW x 235mmD. Lam Module: 12.75" H x 12.25" W x 9.25" D / 324mmH x 313mmW x 235mmD.
Weight	HDP5000: 16 lbs. / 7.3 kg, HDP5000 + Dual-Sided Module: 22 lbs. / 10 kg, HDP5000 + Single-Sided Lam Module: 28 lbs. / 12.7 kg. HDP5000 + Dual-Sided Module + Dual-Sided Lam Module: 36 lbs. / 16.4 kg.
Agency Listings	Safety: UL 60950, CSA C2.2 No 60950, CB report (EN 60950), and CE mark EMC: FCC Part15 Class A, EN 55022: 1998 Class A, CRC c1374, EN 61000-3-2: 2000, EN 61000-3-2: 1995, EN 55024: 1998, CE mark, and CCC mark.
Supply Voltage	100-240 VAC, 3.8A.
Supply Frequency	50 Hz / 60 Hz.
Warranty	Printer – Two years, including one year of free printer loaner support (U.S. only); optional Extended Warranty Program (U.S. only). Printhead – Lifetime; unlimited pass.
FARGO Secure Materials	FARGO Card Printer/Encoders require highly specialized media to function properly. To maximize printed card quality and durability, printhead life, and printer/encoder reliability, use only FARGO Secure Materials. FARGO warranties are void, where not prohibited by law when non-FARGO Secure Materials are used.
Options	Card Lamination Module – single-sided or dual-sided (simultaneous)*** • Magnetic stripe encoding • 200-card input hopper. Smart card encoding (contact/contactless) • Dual-sided printing • Door and cartridge locks Printer cleaning kit. Secure Proprietary Consumables System • Custom Secure Holographic HDP Film and Overlamine.
Software	FARGO Workbench Diagnostic Utility.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 33 of 430

Specifications	Description
* Indicates the ribbon type and the number of ribbon panels printed where Y=Yellow, M=Magenta, C=Cyan, K=Resin Black, I=Inhibit, F=Fluorescing, H=Heat Seal. ** Print speed indicates an approximate print speed and is measured from the time a card drops into the output hopper to the time the next card drops into the output hopper. Print speeds do not include encoding time, or the time needed for the PC to process the image. The processing time is dependent on the size of the file, the CPU, amount of RAM, and the amount of available resources at the time of the print. *** ABS and PVC cards are not recommended for use in the HDP5000 Lamination Module. (Free card proofing available. Please contact your local integrator for more information). **** Linux versions: Ubuntu 7.10, Red Hat Enterprise Desktop 5, Fedora Core 7, Fedora Core 8, openSUSE 10.3.	

Refer to Appendix E: Datasheets, "HNL-60126 06.00-23- 4C049 HID HDP5000.pdf."

2.1.2.4 ID Badge Camera - SoftwareHouse 20K758USB-SYS

The Videology 20K758USB-SYS High-resolution color camera with a desk-mounted stand has been selected to capture images for user ID checks at key access points and /or for ID badge production.

Features:

- CCD sensor provides high sensitivity and quality
- Still image capture with streaming video
- Flexible gooseneck arm allows for easy camera control
- Small footprint saves tablespace
- USB 2.0 bus provides power and camera control
- Software
- USB 2.0 viewer software and Microsoft Digitally
- Certified WDM Device Drivers for 32bit and 64bit
- Windows operating systems
- DirectX/DirectShow compliant
- TWAIN-compliant



Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 34 of 430

Figure 10. ID Badge Camera - 20K758USB-SYS

[Table 3](#) provides a list of specifications for the ID badge camera.

Table 3. ID Badge Camera - SoftwareHouse 20K758USB-SYS

Specifications	Description
Electrical	
Image Sensor	1/4" IL CCD.
Active Pixels	752 x 582.
Viewer Display	720 x 576 pixels max (USB 2.0, 30fps).
Sensitivity	< 0.5 Lux.
Signal To Noise Ratio	> 48 dB (AGC off).
Gamma	0.45 default (1.0 via Software). Gain Control.
Gain Control	Automatic 36 dB (AGC default) or Fixed options via software.
Scan Mode	Interlaced / Non-Interlaced (selectable via Software).
Mirror Mode	Yes (horizontal/vertical).
Synchronization	Internal.
Back Light Compensation	Default on (selectable via software).
White Balance Mode	AWB auto white mode, Fixed modes selectable via software.
Contour Enhancement	Default on.
Iris Control	CCD Iris default.
Shutter Speeds	Automatic. 14 fixed speeds via software 1/6.5 - 1/100,000.
Control Communication	Camera control via USB bus.
Video Output	USB 2.0.
Power Supply	5VDC via USB bus.
Power Consumption	< 1.3 W.
Environmental	
Operating Temp.	-15° C to + 55° C.
Operating Humidity	20% up to 93% RH.
Storage Temp.	-25° C to + 70° C.
Storage Humidity	Up to 98% RH.
Mechanical	
Dimensions (WxHxD)	13.2cm x 52cm x 12cm (from center of camera to bottom of base).
Weight	2.1kg.
Cable	Integrated 8.2 ft USB cable.
Lens	Fixed 6mm f2.0 (30S0620N-IR).
Lens Mount	CS.
Software	

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 35 of 430

Specifications	Description
Viewer (included) SFT-07019	WDM device drivers. DirectX/DirectShow compliant. TWAIN-compliant (requires driver installation).
Recommended System Requirements	
Hardware	Pentium IV 2.3GHz +, 1GB hard drive, Intel USB 2.0 Host controller.
Software	Windows 7 32 bit and 64 bit. Windows Vista 32 bit and 64 bit. Windows XP Service pack 2 +, DirectX 9.0c or above.

Refer to Appendix E: Datasheets, "HNL-60126 06.00-22- 4C048 SWHOUSE 20K758USB-SYS.pdf."

2.1.2.5 Signature Pad - Topaz Systems SigLit LCD 1x5 T-L (BK) 460

The Topaz SigLite® LCD 1x5 is a small electronic signature capture pad with a transfective LCD that displays "electronic ink" under the pen tip during a signing. Bundled secure software APIs provide for interactive text, graphics, and pen-tap hotspots and checkboxes, which enable users to navigate screens and select preferred options.



Figure 11. Signature Pad - Topaz Systems SigLit

[Table 4](#) provides a list of specifications for the signature pad.

Table 4. Signature Pad - Topaz Systems SigLit

Specifications	Description
General Information	
Product Type	Signature Pad
Brand Name	Topaz
Manufacturer	Topaz Systems, Inc.
Product Model	T-S460.
Product Name	SigLite T-S460 Electronic Signature Capture Pad
Product Line	SigLite
Technical Information	
Pad Resolution	410 ppi.
Signing Area	4.30" x 1.40."

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 36 of 430

Specifications	Description
Warranty	
Limited Warranty	1 Year
Input Devices	
Input Device Type	Active Pen
Interfaces/Ports	
Host Interface	USB.
Other	
Green Compliant	Yes
Green Compliance Certificate/Authority	RoHS

2.1.2.6 Printer - HP LaserJet Inkjet Printer (712D)

The OCC workstation attendant can print a document to an HP 712D LaserJet inkjet printer, which has the following features.

- Hardware integration pocket for solution integration (HIP)
- Intuitive 4-line color display with 10-button keypad
- Easy-access USB port to print files directly
- Built-in automatic two-sided printing
- Two 250-sheet input trays for letter and legal-size media
- 100-sheet multipurpose tray 1 handles heavy custom media up to 199 g/m²
- 500-sheet input tray for a 1,100 total input capacity
- 250-sheet output bin
- HP Jetdirect Gigabit Ethernet print server
- Hi-Speed USB 2.0 printing port
- Hi-Speed USB 2.0 port (for connecting third-party devices)
- 800 MHz processor, 512 MB standard memory
- HP High-Performance Secure Hard Disk

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 37 of 430



Figure 12. HP LaserJet Enterprise 700 M712xh Printer

[Table 5](#) provides a list of specifications for the signature pad.

Table 5. HP LaserJet Enterprise 700 M712xh Printer

Specification	Description
Model	HP LaserJet Enterprise 700 Printer M712dn.
Product number	CF236A.
Control panel	5.08 cm, 4-line LCD (color text and graphics); job control buttons; LED status indicators; 10-button keypad, Hardware Integration Pocket; easy-access USB.
Print technology	Laser.
Print speed ¹	Black (A4, normal): Up to 41 ppm. Black (A4, duplex): Up to 26 ppm.
First page out	Black (A4, ready): As fast as 10.5 sec.
Print resolution	Black (best): Up to 1200 x 1200 dpi. Technology: HP Pores 1200, HP Faster's 1200, HP REt, 600 dpi, 300 dpi.
Monthly duty cycle	Up to 100,000 pages A4. Recommended monthly page volume: 5000 to 20,000.
Printer smart software features	HP ePrint, Apple AirPrint™, Mopria-certified, HP Auto On/Auto Off Technology, FutureSmart Firmware, Hardware Integration Pocket, Easy Access USB.
Standard print languages	HP PCL 6, HP PCL 5, HP postscript 3 emulation, native PDF printing (v 1.4).
Print area	Print margins Top: 2 mm, Bottom: 2 mm, Left: 2 mm, Right: 2 mm.
Duplex printing	Automatic (standard).
Processor speed	800 MHz.
Standard Connectivity	2 Hi-Speed USB 2.0. 1 Hi-Speed USB 2.0 Device. 1 Gigabit Ethernet 10/100/1000 Base-T.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 38 of 430

Table 5. HP LaserJet Enterprise 700 M712xh Printer

Specification	Description
	1 Hi-Speed USB 2.0 Easy Access Walkup Port. 1 Hardware Integration Pocket (HIP).
Optional	802.11b/g/n wireless LAN (station mode), other networking accessories, HP Jetdirect 2700w USB Wireless Print Server.
Wireless	Optional, enabled with purchase of a hardware accessory.
Mobile printing capability	HP ePrint; Apple AirPrint™; Mopria™-certified.
Supported network protocols	IPv4/IPv6: Apple Bonjour Compatible (Mac OS v10.2.4 or higher), SNMPv1/v2c/v3, HTTP, HTTPS, FTP, TFTP, Port 9100, LPD, WS Discovery, IPP, Secure-IPP, IPsec/Firewall; IPv6: DHCPv6, MLDv1, ICMPv6; IPv4: Auto-IP, SLP, Telnet, IGMPv2, BOOTP/DHCP, WINS, IP Direct Mode, WS Print.
Network capabilities	Yes, via HP Jetdirect Ethernet embedded print server (standard) supports: 10Base-T, 100Base-Tx, 1000Base-T; 802.3az (EEE) support on Fast Ethernet and Gigabit. Ethernet; IPsec (standard); 802.11b/g/n wireless networking (optional).
Hard disk	Standard: 8 GB Solid State Drive (SSD).
Memory	Standard: 512 MB; Maximum: 1 GB.
Number of paper trays	Standard: 3. Maximum: 6.
Media types	Paper (color, letterhead, light, plain, preprinted, pre-punched, recycled, rough, tough paper), bond, cardstock, envelope, labels, transparency, vellum.
Media size	Custom (metric): Tray 1: 76.2 x 127 to 312 x 469.9 mm; Tray 2: 148 x 210 to 297 to 363 mm; Tray 3: 148 x 210 to 297 to 431 mm. Supported (metric): Tray 1, 2: A3; A4; A5; B4 (JIS); B5 (JIS); Tray 3: A3; A4; A5; B4 (JIS); B5 (JIS).
Media weight	Tray 1: 60 to 199 g/m²; Tray 2, 3: 60 to 120 g/m².
Input capacity	Tray 1: sheets: 100; envelopes: 10; labels: 100 transparencies: 100; postcards: 10. Tray 2: sheets: 250. Tray 3: sheets: 250. Maximum: Up to 4,600 sheets (CF239A (1x) and CF243A can be installed together; No other input accessories can be combined).
Output capacity	Standard: Up to 250 sheets. Envelopes: Up to 50 envelopes. Transparencies: Up to 250 sheets. Maximum: Up to 250 sheets.
Compatible operating systems	Windows 10, Windows 8, Windows 7, Windows Vista, Windows Server 2008 (32-bit/64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2003 (SP1+); Mac OS X v10.6, v10.7
Minimum system requirements	Windows: Windows 10, Windows 8, Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows Server

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 39 of 430

Table 5. HP LaserJet Enterprise 700 M712xh Printer

Specification	Description
	2003 (SP1+): 200 MB available hard disk space (for OS-compatible hardware system requirements, see http://www.microsoft.com) Mac: Mac OS X v10.6, v10.7; 200 MB available hard disk space; operating system compatible hardware system requirements, see apple.com.
Software included	Windows Installer, HP PCL 6 discrete driver, Mac Installer, HP Postscript emulation driver.
Security management	Management security: SNMPv3, SSL/TLS, WPA2-Enterprise, 802.1X authentication (EAP- PEAP, EAP-TLS), IPP over TLS, IPsec/Firewall with Certificate, Pre-Shared Key Authentication, and Kerberos Authentication; Support for WJA-10 IPsec Configuration using IPsec Plug-in.
Printer management	HP Web Jetadmin, HP Utility (Mac).
Printer dimensions (W x D x H)	Minimum: 568 x 596 x 392 mm. Maximum: 858 x 989 x 392 mm.
Package dimensions (W x D x H)	810 x 785 x 644 mm.
Printer weight	38.5 kg.
Package weight	45.6 kg.
Operating environment	Temperature: 10 to 32.5°C. Humidity: 30 to 70% RH.
Storage conditions	Temperature: 0 to 60°C. Humidity: 10 to 90% RH.
Acoustics	Acoustic power emissions: 6.8 B(A). Acoustic pressure emissions: 54 dB(A).
Power	Requirements: Input voltage: 220 to 240 VAC (+/- 10%), 50/60 Hz (+/- 2 Hz). Consumption: 786 watts (printing), 22.1 watts (ready), 6.1 watts (sleep), 0.21 watts (off). Typical Electricity Consumption (TEC): 3.289 kW/Week. Typical Electricity Consumption (TEC): 2.95 kWh/Week. Power supply type: Built-in power supply.
Energy savings feature technology	HP Auto-On/Auto-Off Technology; Instant-on Technology.
Certifications	CISPR 22:2008 / EN 55022:2010 (Class A); EN 61000-3-2 :2006 +A1:2009 +A2:2009; EN 61000-3-3 :2008; EN 55024:1998 +A1 +A2; EMC Directive 2004/108/EC with CE Marking (Europe); other EMC approvals as required by individual countries. ENERGY STAR® qualified; EPEAT® Silver; CECP. Blue Angel compliant No; Please refer to the ECI document.
Country of origin	Made in China.
What's in the box	HP LaserJet Enterprise 700 M712dn; HP Black LaserJet Toner Cartridge (~10,000 pages); Automatic duplexer for two-sided printing;

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 40 of 430

Table 5. HP LaserJet Enterprise 700 M712xh Printer

Specification	Description
	Getting Started Guide, CD containing drivers and electronic documentation; Power cord.
Warranty	One-year, next-business day, onsite warranty. Warranty and support options vary by product, country, and local legal requirements. Go to http://www.hp.com/support to learn about HP award-winning service and support options in your region.

Refer to Appendix E: Datasheets, "HNL-60126 06.00-41-4CO69- HP LaserJet Ink Printer 712D.pdf."

2.2 ACS HARDWARE

This section lists the ACS components and provides some specifications.

2.2.1 Access Card - HID 1386-LGGMN ISOProx II

The RF-programmable ISOProx II proximity access card provides proximity technology and photo identification on a single access control card.



Figure 13. Access Card - HID 1386-LGGMN ISOProx II

Features:

- Offers an extremely consistent read range. Unaffected by body shielding or variable environmental conditions, even when close to keys or coins.
- Can be carried with credit cards in a wallet or purse. Use with a strap and clip as a photo ID badge
- Print directly to the card with a direct image or thermal transfer printer. Slot punch vertically or horizontally for easy use
- Cross-reference list correlating the external card number, and the programmed ID number is provided for easy system administration
- Offers 137 billion unique codes
- Passive no-battery design allows for an infinite number of reads
- Strong, flexible, and resistant to cracking and breaking
- Lifetime warranty against defects in materials and workmanship

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 41 of 430

Table 6. Access Card - HID 1386-LGGMN ISOProx II

Specifications	Description
Dimensions	2.125" x 3.370 x 0.030" +/- nominal (5.4 x 8.6 x 0.076 +/- 0.0076 cm).
Card Construction	Thin, flexible polyvinyl chloride (PVC) laminate.

2.2.2 Proximity Card Reader - HID Proximity Card System 1

HID cards, also called prox cards, proximity cards, and access control cards, are cards that use RFID embedded technology. HID card readers are used in access control systems to open doors.

2.2.3 SmartCard Reader - HID 920P MultiClass SE Readers

The HID Global's iCLASS SE platform smart card is a secure, standards-based flexible platform that is highly adaptable, interoperable, and a secure access control solution.


Figure 14. SmartCard Reader - HID 920P MultiClass SE Readers

[Table 7](#) provides a list of specifications for the signature pad.

Table 7. SmartCard Reader - HID 920P MultiClass SE Readers

Specifications	Description
Base Part Number	920P.
Typical Read Range* (inches)	iCLASS SE: 3.5" (8.9 cm). SE for DESFire® EV1: 1.6" (4.1 cm). SE for MIFARE Classic: 2.7" (6.9 cm).
Mounting	Wall Switch Size; designed to mount and cover single gang switch boxes primarily used in the Americas and includes a slotted mounting plate for European and Asian back box spacing.
Color	Black or Gray.
Keypad	No.
Dimensions	3.3" x 4.8" x 1.0." 8.4 cm x 12.2 cm x 2.4 cm.
Product Weight (Pigtail)	7.8oz (222g).
Product Weight (Terminal Strip)	7.6oz (216g).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 42 of 430

Table 7. SmartCard Reader - HID 920P MultiClass SE Readers

Specifications	Description
Operating Voltage Range	5-16 VDC, Linear supply recommended.
Current Draw - Standard Power Mode*** (mA)	110.
Current Draw - Intelligent Power Management (IPM) Mode*** (mA)	50.
Peak Current Draw - Standard Power or IPM Mode*** (mA)	265.
NSC** Power Consumption - Standard Power Mode (W @ 16VDC)	1.8.
NSC** Power Consumption - w/ IPM (W @ 16VDC)	0.8.
Operating Temperature	-31° to 150° F (-35° to 65° C).
Storage Temperature	-67° to 185° F (-55° to 85° C).
Operating Humidity	5% to 95% relative humidity non-condensing.
Environmental Rating	IP55.
Transmit Frequency	13.56 MHz & 125 kHz.
13.56 MHz Card Compatibility	Secure Identity Object™ (SIO®) on iCLASS SE/SR, SE for MIFARE DESFire EV1, and SE for MIFARE Classic (On by Default). Non-default programmable options include: additionally support. - standard iCLASS Access Control Application (order with Standard interpreter). -ISO14443A (MIFARE) CSN, ISO14443B CSN, ISO15693 CSN. - Mifare and Mifare DESFire EV1 custom data models.
125 kHz Card Compatibility†	HID Prox, AWID, Indala, EM4102.
Communications	Optional OSDP with SCP over RS485. Wiegand/Clock-and-Data Interface 500ft (150m) (22AWG) - Use Shielded cable for best results.
Panel Connection	Pigtail or Terminal Strip.
Certifications	UL294/cUL**** (US), FCC Certification (US), IC (Canada), CE (EU), C-tick (Australia, New Zealand), SRRC (China), MIC (Korea), NCC (Taiwan), iDA (Singapore), RoHS, FIPS-201 Transparent FASC-N Reader.
Crypto Processor Hardware Common Criteria Rating	EAL5+.
Patents	US7180403, US7439862, US7124943, US5952935, US6058481, US6337619.
Housing Material	UL94 Polycarbonate.
Manufactured with % of recycled content (Pigtail)	10.5%.
Manufactured with % of recycled content (Terminal Strip)	11.0%.
UL Ref Number	RP40E.
Warranty	Limited Lifetime.
* Typical read range achieved in air. Different types of metal will cause some degradation (typically up to 20%).	

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 43 of 430

Table 7. SmartCard Reader - HID 920P MultiClass SE Readers

Specifications	Description
Use spacers to space product off metal and improve read range if required.	
** NSC = Normal Standby Current.	
*** Measured in accordance with UL294 standards.	
**** UL294 functionally certified for Wiegand output only.	
† If a technology read range is not listed, the compatibility is not currently available in the associated reader model.	

Refer to Appendix E: Datasheets, “HNL-60126 06.00-11- 4C012 HID 920P multiCLASS SE Readers.pdf.”

2.2.4 In/Out Module - Genetec Mercury Security MR-16IN I/O Module

Genetec Mercury Security MR-16 is 16-Zone Input/Output Module. Genetec Synergis™ supports Mercury Security’s open field hardware enabling HART to deploy industry-standard access control modules.

The MR16IN 16-input interface module supports 16 general-purpose input circuits. Supporting a range of wired and wireless reader technology, the MR16IN is managed by a Mercury Security EP1502, EP2500, and EP4502 controller through a high-speed RS-485 network and ultimately, the Synergis Cloud Link appliance over IP.

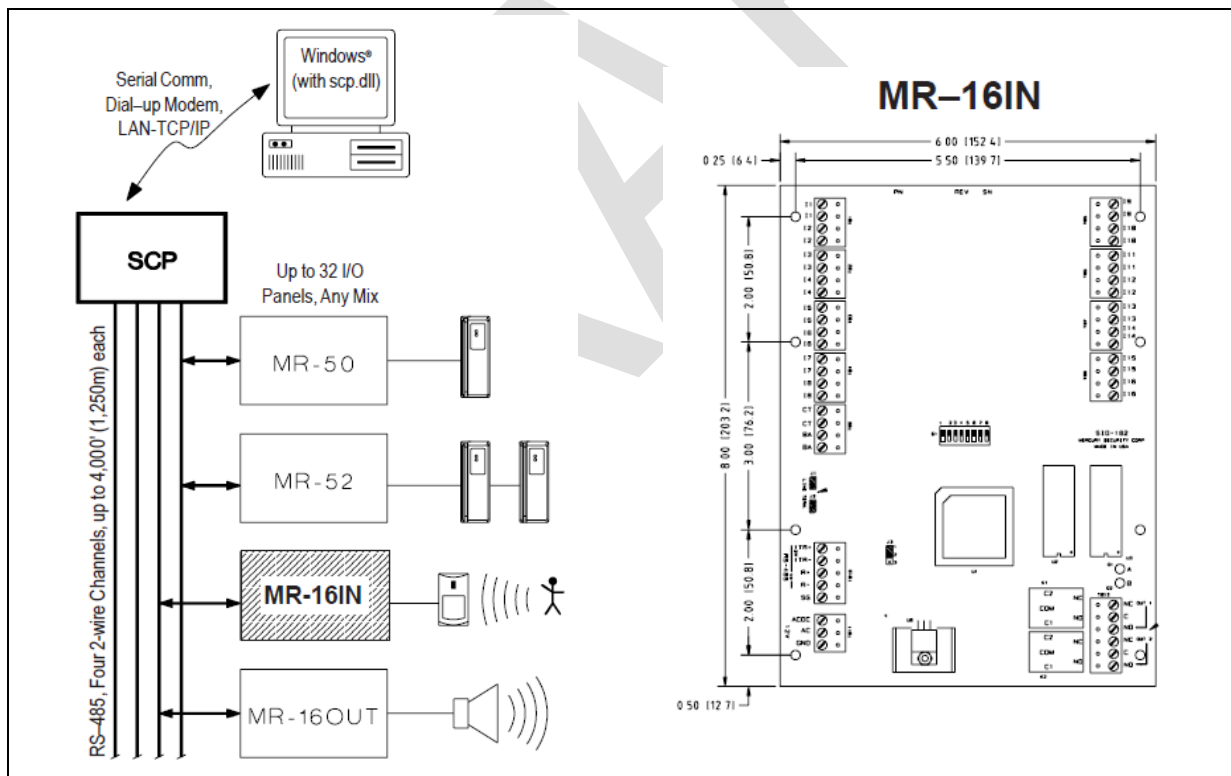


Figure 15. In/Out Module - Genetec Mercury Security MR-16IN I/O Module

Table 8 provides a list of specifications for the MR-16N I/O module.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 44 of 430	

Table 8. In/Out Module - Genetec Mercury Security MR-16IN I/O Module

Specifications	Description
Electrical	
Primary Power	12 VDC +/- 15%, 350 mA. 12 VAC +/- 15%, 600 mA RMS.
Communication	RS-485, 2-wire/4-wire, 4,000'. (twisted pair w. shield, Belden 9541/9542).
Inputs	16 General purpose: programmable circuit type 2 Dedicated: Tamper and Power Monitor.
Outputs	2 Relays: Form-C, 5 Amp 30 VDC.
Mechanical	
Dimensions	6.0' W x 8.0' L x 1.0' H, (152mm W x 203mm L x 25mm H).
Environmental	
Temperature	0—70 °C operational, -55—85 °C storage.
Humidity	0 to 95% RHNC.

Refer to Appendix E: Datasheets, "HNL-60126 06.00-2- 4C002 Genetec Mercury Security MR-16IN.pdf."

2.2.5 In/Out Module - Genetec Mercury Security MR-16OUT Module

The MR-16OUT will interface sixteen output control relays to an Access Control and Security Monitoring System through an SCP (System Control Processor).

Relays are often used for status annunciation and for general facility control, such as lighting, heating/cooling and door control. Relay operation may be initiated by direct operator commands, by time schedules, or by event-based procedures.

The relays can be configured for a failsafe or fail secure operation. The relays support "On," "Off," "Pulse," and "Repeating Pulse" commands. A pulse may range from .1 second to over 24 hours.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 45 of 430	

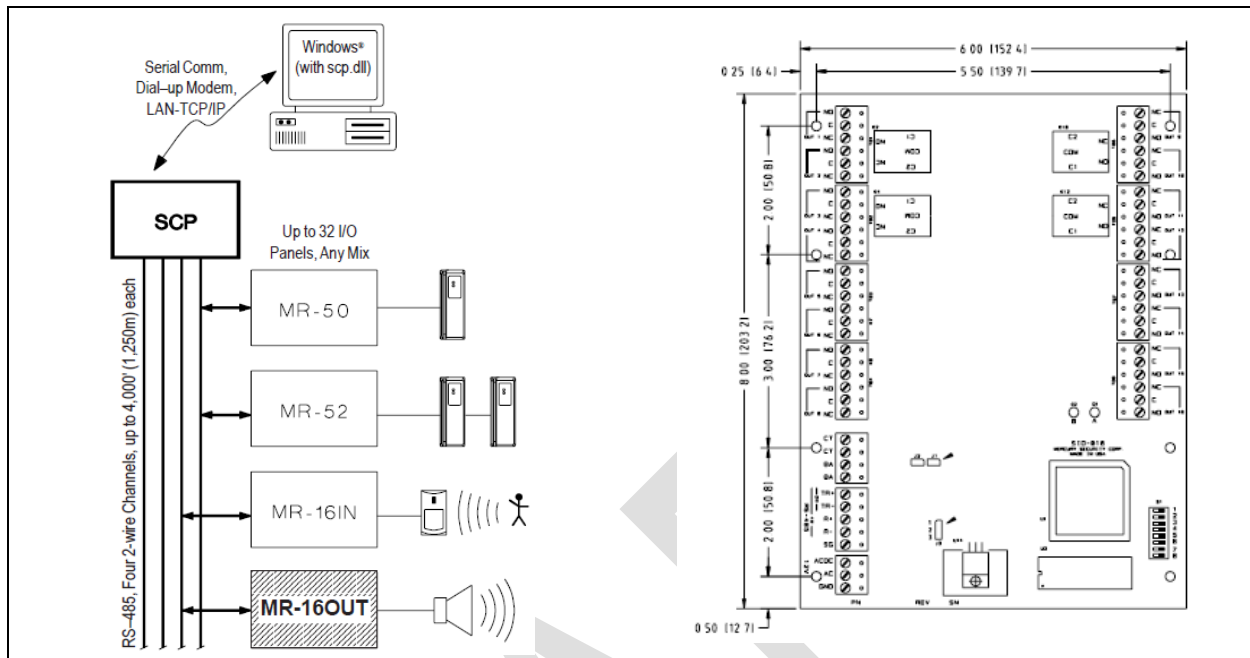


Figure 16. In/Out Module - Genetec Mercury Security MR-16OUT Module

Table 9 provides a list of specifications for the MR16OUT module.

Table 9. In/Out Module - Genetec Mercury Security MR-16OUT Module

Specifications	Description
Electrical	
Primary Power	12 VDC +/- 15%, 350 mA. 12 VAC +/- 15%, 600 mA RMS.
Communication	RS-485, 2-wire/4-wire, 4,000'. (twisted pair w. shield, Belden 9541/9542) (twisted pair w. shield, Belden 9541/9542).
Inputs	2 Dedicated: Tamper and Power Monitor.
Outputs	16 Relays: Form-C, 5 Amp 30 VDC.
Mechanical	
Dimensions	6.0' W x 8.0' L x 1.0' H, (152mm W x 203mm L x 25mm H).
Environmental	
Temperature	0—70 °C operational, -55—85 °C storage.
Humidity	0 to 95% RHNC.

Refer to Appendix E: Datasheets, "HNL-60126 06.00-3- 4C003 Genetec Mercury Security MR-16OUT.pdf."

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 46 of 430	

2.2.6 In/Out Module - Genetec Mercury Security MR-52 I/O Module

16-Zone Input/Output Module.

The MR-52 will interface two card readers, eight general-purpose input monitor points, and six control relays to an Access Control and Security Monitoring System through an SCP (System Control Processor).

The MR-52's two reader ports support magnetic, Wiegand, and proximity readers. Keypads and integrated keypad readers are also supported. Hardware interface and card format settings are loaded through software commands.

The inputs and the relays may be assigned to door related functions or to general-purpose I/O. The inputs support normally open, normally closed, supervised, and non-supervised circuits. End-of-line (EOL) resistance values are configurable. The relays can be configured for fail-safe or fail-secure operation.

The MR-52 passes access requests and status change information to the SCP for processing. When not connected to an SCP, the MR-52 is capable of locally processing access requests based on facility code verification. Up to eight facility codes may be active in each MR-52.

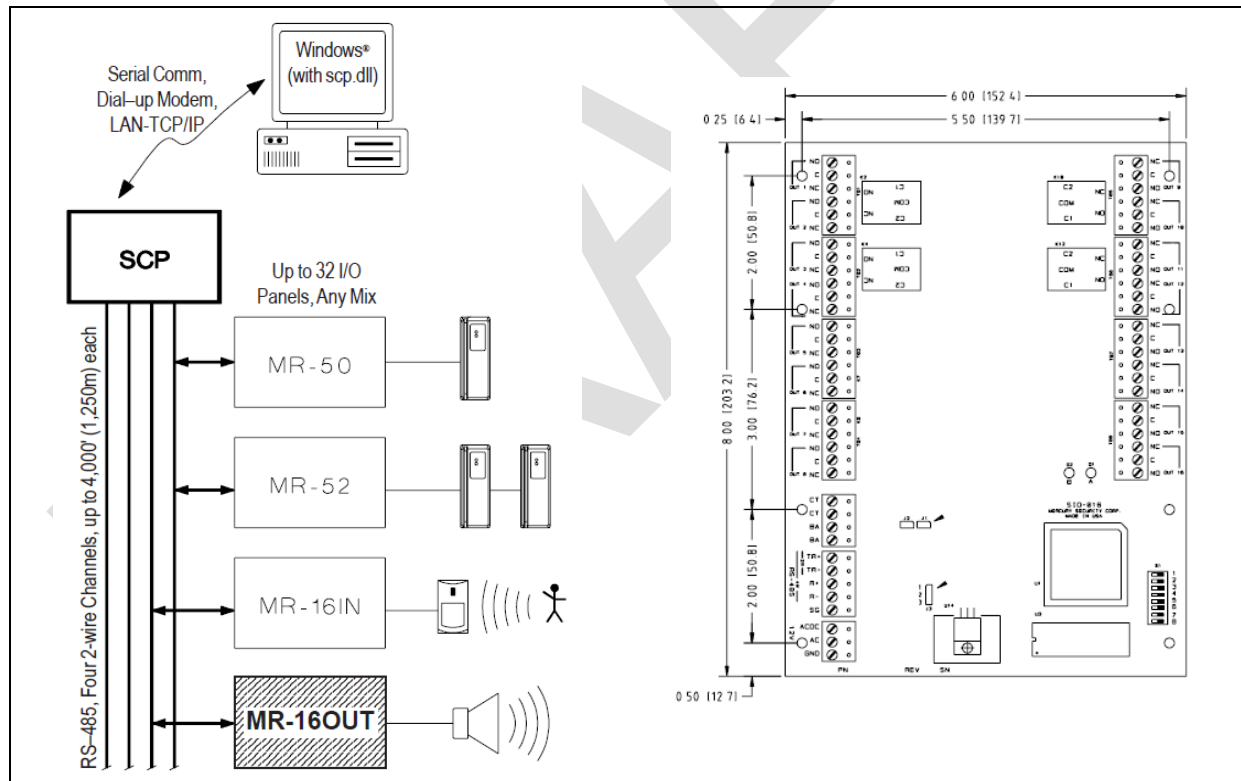


Figure 17. In/Out Module - Genetec Mercury Security MR-52 I/O Module

Table 10 provides a list of specifications for the MR-52 I/O module.

Table 10. In/Out Module - Genetec Mercury Security MR-16OUT Module

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 47 of 430	

Specifications	Description
Electrical	
Primary Power	12 VDC +/- 15%, 350 mA 12 VAC +/- 15%, 600 mA RMS
Communication	RS-485, 2-wire/4-wire, 4,000' (twisted pair w. shield, Belden 9541/9542) (twisted pair w. shield, Belden 9541/9542).
Reader Ports	2 Reader Ports.
Power Regulated	+5 or +12 VDC at 70 mA.
Card	Two wires: Clock/Data or Data-1/Data-0.
Keypad	Multiplexed with card data.
LED	Two-wire or one-wire bi-color LED support.
Buzzer	Only with 'one-wire' LED.
Inputs	2 Dedicated: Tamper and Power Monitor.
Outputs	16 Relays: Form-C, 5 Amp 30 VDC.
Mechanical	
Dimensions	6.0' W x 8.0' L x 1.0' H, (152mm W x 203mm L x 25mm H).
Environmental	
Temperature	0—70 °C operational, -55—85 °C storage.
Humidity	0 to 95% RHNC.

Refer to Appendix E: Datasheets, “HNL-60126 06.00-4- 4C004 Genetec Mercury Security MR-52.pdf.”

2.2.7 Telephone Entry Pad - Ameristar Gate 1837AGS

The Ameristar Gate 1837AGS is suited for complete access control for up to 48 entry points. It provides access control into and within HART facilities.



Figure 18. Telephone Entry - Ameristar Gate 1837AGS

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 48 of 430

Table 11 provides a list of specifications for the telephone entry pad.

Table 11. Telephone Entry - Ameristar Gate 1837AGS

Specifications
Mechanical
Stainless Steel Faceplate.
Galvanized Steel Sub-Plate.
Metal Keypad, with Internally lit LED Keypad and A-Z-CALL Buttons.
Offset Speaker Holes for protection.
Hands-Free Voice Operation (Optional handset available on surface or flush mount only).
Built-In Postal Lock provision, EEPROM memory.
Surface, Flush or Wall mounting styles Flush mount requires Flush Mounting Kit Enclosures are rated NEMA 4x.
Connection Methods
Cellular (powered by AT&T 4G LTE).
VoIP (select DK VoIP or your own VoIP provider).
POTS (Plain Old Telephone Service).
Connection methods noted will incur additional cost for required hardware and/or service subscriptions.
Specifications
Eight Line 20-character Super-Twist LCD Display (1/2 inch characters).
16 VAC (2 Power Transformers included).
Full Duplex Voice Communication.
Stores up to 3000 Phone Numbers, 255 Area Codes.
Max 8000 Weigand Device (card codes), 10 Facility Codes.
10 Facility Codes.
Transaction Buffer stores last 8000 Events.
Control 3 Entry Points, expandable to 48 with Tracker Expansion Boards.
Programmable Directory Codes (1 to 4 digits).
10 & 11-Digit Dialing Capability.
31 Security (permission) Levels, 29 Programmable with 4 Time Zones each.
32 Holiday Schedules.
4-Digit Entry Codes.
Built-In Clock / Calendar.
8 Hold Open Time Zones.
Entry Code Time Zones.
True Anti-Pass Back.
Live Transactions feature (requires TCP/IP internet connection or RS-232 connection).
Miscellaneous
Environmental: 10°F to 145°F (-12°C to 62°C).
Heater Kit (P/N 2600-584) recommended when temperatures routinely fall below 10°F (-12°C).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 49 of 430

Specifications

ADA Compliant Handset Kit (P/N 1807-012) available on Surface or Flush Mount only.

Camera Ready: Optional B&W or Color CCTV Camera. May require additional CCTV equipment.

Shipping weight approximately 20-25 lb (9-11 kg).

Refer to Appendix E: Datasheets, "HNL-60126 06.00-17- 4C024 Ameristar Gate 1837AGS Telephone Entry.pdf."

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 50 of 430	

2.2.8 Request to Exit Detector and TP160 Trim Plates - Bosch DS150i

The DS150i Series consists of the DS150i Detector (light gray) and the DS151i Detector (black). They are specifically designed for Request-to-exit (REX) applications. The DS150i and DS151i detect motion in their coverage area and signal an access control system or door control device.



Figure 19. Request to Exit Detector and TP160 Trim Plates - Bosch DS150i

[Table 12](#) provides a list of specifications for the Bosch DS150i.

Table 12. Request to Exit Detector and TP160 Trim Plates - Bosch DS150i

Specifications	Description
Electrical	
Current Draw	26 mA at 12 VDC.
Voltage ¹²	12 VAC or VDC; 24 VAC or VDC.
Mechanical	
Alarm Output	Two Form C relay contacts.
Indicators	One activation LED.
Relay Latch Time	Adjustable to 60 sec.
Enclosure Dimensions	3.8 cm x 15.9 cm x 3.8 cm (1.5 in. x 6.25 in. x 1.5 in.).
Enclosure Material:	High impact ABS plastic enclosure.
Power Loss Default Mode	Programmable fail-safe or fail-secure modes.
Timer Mode	Programmable reset (accumulative) or non-reset (counting) mode.
Mounting Location	Surface mount on wall or ceiling.
Environmental	
Operating Temperature	-29°C to +49°C (-20°F to +120°F).
Radio Frequency Interference (RFI) Immunity:	No alarm or setup on critical frequencies in the range from 26 MHz to 1000 MHz at 50 V/m.
Certifications and approvals	
Europe	CE 2004/108/EC EMC Directive; 2006/95/EC Low-Voltage Directive;

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 51 of 430

Specifications	Description
	2011/65/EU Restriction of the use of certain hazardous substances in electrical and electronic equipment.
USA	UL ALVY: Access Control Systems Units (UL294).

Refer to Appendix E: Datasheets, "HNL-60126 06.00-17- 4C024 Ameristar Gate 1837AGS.pdf."

2.2.9 Sliding Shelf/Tray - Atlas Sound VTD1 16

Sliding shelf/tray for cabinets for front and read mtg rails.

The versatile shelf can be used upside-down as a tray with a protective lip or right-side-up as a shelf. The unit provides easy access to 16-3/4 wide (max) keyboards, videotape recorders, and control equipment. Solid bearing slides extend 17" outside of cabinet rails and includes lock-out protection. It mounts 19" W cabinets that are 18-1/2" to 25-1/2" deep, which are equipped with front and rear mounting rails. The 16-ga. CRS assembly is finished in black epoxy. It supports up to 85 lbs. (38.56kg) and includes necessary hardware.



Figure 20. Sliding Shelf/Tray - Atlas Sound VTD1 16

Refer to Appendix E: Datasheets, "HNL-60126 06.00-5- 4C005 Atlas Sound VTD1-16.pdf."

2.2.10 Recessed Steel Door Contact - GE 1076D

The GE Interlogix 1078 Series Steel Door contacts are designed specifically for use in the steel doors commonly found in commercial building applications.



Figure 21. Recessed Steel Door Contact - GE 1076D

[Table 13](#) provides a list of specifications for the GE Interlogix steel door contacts.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 52 of 430

Table 13. GE Interlogix 1078 Series Steel Door Contacts

Specifications	Description
Voltage	100V AC/DC max
Current	0.5 A max.
Power 7.5 W max.	7.5 W max.

Refer to Appendix E: Datasheets, “HNL-60126 06.00-9- 4C010 GE 1076D Recessed Door Contact.pdf.”

2.2.11 Industrial Surface Mount Contact - Sentrol 1045 Position Sensors

The 1045 Series industrial contacts protect openings such as metal entry/exit doors, overhead doors, roof hatches, or hinged skylights.


Figure 22. Industrial Surface Mount Contact - Sentrol 1045 Position Sensors

[Table 14](#) provides a list of specifications for the Sentrol position sensors.

Table 14. Industrial Surface Mount Contact - Sentrol 1045 Position Sensors

Specifications	Description
Electrical, 1045W	Voltage: 100 VAC/DC max. Current: 0.5 A max. Power: 7.5 W max.
Features, 1045W	Loop type: Closed. Electrical configuration: Normally open. Gap distance: Up to 1-1/4 in. Lead type: 2 ft. jacketed #22 A.W.G.
Physical	Dimensions: (LxWxD): 3.90 x 0.6 x 0.7 in. (99 x 15 x 18 mm). Construction: Flame-retardant ABS plastic. Color: White (1045W available in gray).
Regulatory	UL.

Refer to Appendix E: Datasheets, “HNL-60126 06.00-10- 4C011 Sentrol 1045 Position Sensors.pdf.”

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 53 of 430

2.2.12 Lock Box - Knox Box Bosch 3262

The 3262 Knox-Box holds keys, access cards, and other small items necessary for emergency access. Refer to Appendix E: Datasheets, “HNL-60126 06.00-13- 4C016 Knox Box 3262.pdf.”



Figure 23. Lock Box - Knox Box Bosch 3262

2.2.13 Key Switch - Camden CM1170-7024

CM-1100 is a single gang (2 3/4”) width; CM-2000 is only 13/4” wide, perfect for door frames or narrow areas. Both models accept one or two switches and have a countersunk cylinder opening, in a one-piece casted assembly. A brass cylinder lock ring, 2 socket/slotted screws, and 2 tamperproof screws with a driver are also supplied. (The mortise cylinder is available separately from CAMDEN DOOR CONTROLS.) The design and construction make it ideal for all-weather environments. The assembly is tamper and vandal resistant.

CM Key Switches are flexible and can be supplied in numerous switch configurations to suit varied commercial and industrial applications, and functions. CAMDEN Key Switches provide a practical, cost-effective means for authorized personnel to control and signal various functions within a complex.



Figure 24. Key Switch - Camden CM1170-7024

[Table 15](#) provides specifications for the key switch.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 54 of 430

Table 15. Key Switch - Camden CM1170-7024

Features	
Single Gang and Narrow Style Models	Accepts Standard Mortise. Cylinders, 1" – 1 1/4."
Heavy-Duty 1/4" Thick Aluminum Plate	1 Piece Die Cast Construction.
Locators Prevent Cylinder from Spinning	Vandal Resistant.
Cylinder Sits Flush to Faceplate	Indoor or Outdoor Applications.
UL/CSA Approved Switches	1 or 2 Switches May Be Installed.
Wide Range of Switch Configurations	Color-Coded 18 AWG Soldered Leads.
Heat Shrink Protective Sleeve Over Contacts	Casted Centre Rib Protects Switches from Damage.
Brushed Aluminum Finish	Custom Color Finishes & Engraving Available.
Optional Led Indicators	Optional 1-60 Second DPST Pneumatic Time Delay.

Refer to Appendix E: Datasheets, "HNL-60126 06.00-15- 4C022 Camden CM1170-7024 Key Switch.pdf."

2.2.14 Magnetic Contacts: Overhead Door - GE 2200A-L

The GE Security 2202 Series overhead door magnetic contact is for use in the rigorous environments of commercial and industrial installations.

The floor mount units are constructed with a low-profile heavy cast aluminum housing. The reed switch assembly is fully encased in GE Security's exclusive polyurethane potting material to prevent damage due to moisture or humidity. A wide operating gap distance of up to 3 inches makes installation easy and helps prevent false alarms caused by door movement or damaged and loose-fitting doors.



Figure 25. Magnetic Contacts: Overhead Door - GE 2200A-L

[Table 16](#) provides specifications for the magnetic contacts.

Table 16. Magnetic Contacts: Overhead Door - GE 2200A-L

Specifications	
Electrical	
Voltage: 100 VAC/DC max.	
Current: 0.5 A max.	

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 55 of 430

Specifications
Power: 7.5 W max.
Physical
Dimensions, 2202A (LxWxD): 3.50 x 1.50 x 1.50 in. (89 x 38 x 38 mm). Dimensions, 2202AU and 2204AU (LxWxD): 3.125 x 2.125 x 0.81 in. (79x 54 x 21 mm). Construction: Cast aluminum. Color: Aluminum.
Regulatory
C-UL-US.

Refer to Appendix E: Datasheets, “HNL-60126 06.00-16- 4C023 GE 2200A-L Overhead Door Magnetic Contacts.pdf.”

2.2.15 Magnetic Contacts: Heavy Duty - Sentrol 2105

The Magnapull™ magnetic pull-apart cords protect valuable free-standing items that are stored outdoors. The high-impact plastic housing protects the contact from corrosion or high resistance buildup. End-users simply insert the cable into the contact housing; there is nothing to line up. An alarm condition is created when the cord with the magnet is pulled from the housing.



Figure 26. Magnetic Contacts: Heavy Duty - Sentrol 2105

[Table 17](#) provides specifications for the magnetic contacts.

Table 17. Magnetic Contacts: Heavy Duty - Sentrol 2105: Specifications

Specifications	Description
Voltage	100 V AC/DC max.
Current	0.5 A max.
Power	7.5 W max.

Refer to Appendix E: Datasheets, “HNL-60126 06.00-18- 4C034 Sentrol 2105 Heavy-Duty Magnetic Contacts.pdf.”

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 56 of 430

2.2.16 Push Button Exit Control - DynaLOCK 6270

SPDT MOM contacts with the illuminated green button. The DynaLOCK 6270 provides a request to exit (REX). Monitoring is accomplished with illuminated indicators.



Figure 27. Push Button Exit Control - DynaLOCK 6270

Table 18 provides the specifications for the DynaLOCK 6270.

Table 18. Push Button Exit Control - DynaLOCK 6270: Specifications

Specifications	Descriptions
Contact Rating	10 Amps @ 125VAC / UL.
Illumination	12/24 VDC.
Terminations	7" Color-Coded 18AWG Leads.
Faceplate	Single-Gang (Double Available).
Finish	US32D Brushed Stainless Steel (Others Available).
Signage	"EXIT" in Black Letters.

Refer to Appendix E: Datasheets, "HNL-60126 06.00-19- 4C035 DynaLOCK 6270 Push Button.pdf."

2.2.17 IP Video Storage - BCDVideo BCD360V8

The BCDVideo Nova Series is manufactured specifically for Enterprise IP Video Surveillance applications. The 1U Management Platform systems are built specifically for those video applications. The BCD360 can be utilized as a management server or as a video recording server where archival storage is either on a direct-attached storage array or centralized storage array.



Figure 28. BCD360V8-M-MP-C

Table 19 provides specifications for the BCD Video IP video storage unit.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 57 of 430

Table 19. BCD360V8-M-MP-C: Specifications

Specifications		Description	
Processor	(1) Intel Xeon E5 Processor (Second Processor Optional)	Form Factor	1U Rack Mount.
Single Processor Passmark	7288	Hard Drives	Enterprise Drives.
Dual Processor Passmark	13613		
RAM	16GB	Hard Drive Bays	8 Bays.
BCDVideo SMARTrecovery	Embedded	Streaming Video Ingestion	Up to 1000Mbit/s.
BCDVideo SMARTvms	Embedded	RAID Controller	Optimized for Video Streaming.
BCDVideo SMARTconnect	Embedded	RAID Level Supported	RAID 1,10,5 or 6.
BCDVideo SMARTcontrol	Embedded	Dimensions (W x H x D)	17.54 x 1.7 x 29.5 in.
Power Supplies	Redundant	Warranty	Lifetime Phone Support 5-Year Global NBD Onsite.

Refer to Appendix E: Datasheets, “HNL-60126 06.00-20- 4C046 BCDVideo BCD360V8.pdf.”

2.2.18 Motion Detector - Bosch ISC-CDL1 & B328

The Commercial Series TriTech motion detectors are designed to ensure reliable catch performance and false alarm immunity in commercial applications. ISCCDL1-W15x detectors use a combination of passive infrared (PIR) and microwave Doppler radar detection technologies with advanced signal processing. New features such as integrated, selectable end-of-line resistors, a self-locking enclosure with integrated bubble level, and a removable lift gate style terminal strip make installation of Commercial Series detectors easier and more reliable.


Figure 29. Motion Detector - Bosch ISC-CDL1 & B328

[Table 20](#) provides the specifications for the Bosch motion detector.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 58 of 430

Table 20. Motion Detector - Bosch ISC-CDL1 & B328: Specifications

Specifications	Description
Properties	
Dimensions	120 mm x 70 mm x 55 mm (4.7 in. x 2.75 in. x 2.2 in.).
Material	High-impact ABS plastic.
Color	White.
Terminal wire size	Ø 0.40 mm to 1.29 mm (26 AWG to 16 AWG) (UL: 22 AWG to 16 AWG).
Environmental	
Environment	Complies with EN50130-5 Environmental Class II.
Relative humidity	93% non-condensing.
Temperature (operating)	-30°C to +55°C (-22°F to +130°F) UL: 0°C to +49°C (+32°F to +120°F) AFNOR/CNPP: -10°C to +55°C.
Electrical	
Current	Standby: <15 mA. Alarm: ≤16 mA maximum.
Voltage (operating)	VDC to 15 VDC.
Radio Frequency Interference (RFI) Immunity	No alarm or setup on critical frequencies in the range from 150 kHz to 2.7 GHz at field strengths less than 10 V/m.
Outputs	
Alarm relay, trouble relay	Solid-state, supervised, normally closed (NC) contacts rated for <100 mA, 25 V, 2.5W.
Tamper	Supervised, normally closed (NC) contacts rated for <100 mA, 25 V, 2.5W.
End-of-line resistors	Alarm: 1.0 k, 2.2 k. Tamper: 1.0 k, 2.2 k, 33 k.

Refer to Appendix E: Datasheets, "HNL-60126 06.00-24- 4C037 Bosch ISC-CDL1 & B328.pdf."

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 59 of 430

2.2.19 DC Rack Mount ACS Power Supply - Altronix R615DC1016

The R615DC1016 provides 6-15VDC distributed via 16 fuse protected outputs for powering CCTV Cameras, heaters, and other video accessories.



Figure 30. DC Rack Mount ACS Power Supply - Altronix R615DC1016

[Table 21](#) provides specifications for the rack mount AC power supply unit.

Table 21. DC Rack Mount ACS Power Supply - Altronix R615DC1016

Specifications	Description
Input: 115VAC, 50/60Hz, 1.9 amp. Output: Sixteen (16) fuse protected outputs. 6-15VDC @ 10 amp total output current. (0.625 amp per device, 3.5 amp max). Outputs are rated @ 3.5 amp. Filtered and electronically regulated outputs. Short circuit and thermal overload protection. Electrical: Operating temperature: 0° C to 49° C ambient. 46.06-76.77 BTU/Hr. System AC input VA requirement: 218.5VA.	Features: Sixteen (16) power LEDs. Illuminated master power disconnect circuit breaker with manual reset. 3-wire grounded line cord. Removable terminal blocks with locking screw flange. Spare fuses provided. Mechanical: 2U rackmount chassis for use in standard EIA 19" rack. Enclosure Dimensions (H x W x D approx.): 3.26" (83mm) x 19.125" (486mm) x 8.5" (216mm). Product weight (approx.): 17.15 lbs. (7.78 kg). Shipping weight (approx.): 18.15 lbs. (8.23 kg).

Refer to Appendix E: Datasheets, "HNL-60126 06.00-6- 4C006 Altronix R615DC1016.pdf."

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 60 of 430

2.2.20 Rack Mount Access Power Controller - Altronix Maximal 33RD

Maximal33RD rack mount access power controller distributes and switches power to access control systems and accessories.

2.2.21 Rackmount Server - BCDVideo BCD320E8-M-SAS-MP-C

The BCDVideo Nova Series is manufactured specifically for Enterprise IP Video Surveillance applications. The 1U Management Platform systems are built specifically for those video applications. The BCD320 can be utilized as a management server or as a video recording server where archival storage is either within the server chassis, within a direct-attached storage array, or centralized storage array.



Figure 31. Rackmount Server - BCDVideo BCD320E8-M-SAS-MP-C

Table 22 provides the specifications for the rackmount server.

Table 22. Rackmount Server - BCDVideo BCD320E8-M-SAS-MP-C

Specifications		Description	
Processor	(1) Intel Xeon E3	Form Factor	1U Rackmount.
Single Processor Passmark	9712	Hard Drives	Enterprise Drives.
RAM	8GB	Hard Drive Bays	4 Bays.
BCDVideo SMARTrecovery	Embedded	Streaming Video Ingestion	Up to 300Mbit/s*.
BCDVideo SMARTvms	Embedded	RAID Controller	Optimized for Video Streaming.
BCDVideo SMARTconnect	Embedded	RAID Level Supported	RAID 0,1,5,6 or 10.
BCDVideo SMARTcontrol	Embedded	Dimensions (W x H x D)	17.54 x 1.7 x 29.5 in.
Power Supplies	Single	Warranty	Lifetime Phone Support 5-Year Global NBD On-site.

Refer to Appendix E: Datasheets, “HNL-60126 06.00-25- 4C056 BCDVideo BCD320E8-M-SAS-MP-C”.pdf.

2.2.22 Rackmount Server - BCDVideo BCD104-170-MP-C

The BCDVideo Nova Series is manufactured specifically for Enterprise IP Video Surveillance applications. The Nova Series is the newest-generation platform utilizing 6G SAS technology, which enables more high-megapixel cameras per system than traditional SATA-based servers. This video recording platform is built with scalability, reliability, and longevity in mind.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 61 of 430



Figure 32. Rackmount Server - BCD104-170-MP-C

Table 23 provides the specifications for the rackmount server.

Table 23. Rackmount Server - BCD104-170-MP-C

Specifications	Description
Form Factor	1U RackMount.
Processor Passmark	9793.
RAM	8GB.
Operating System	Server 2012 R2.
Network Ports	1GbE Ports - QTY 2.
Hard Drive Bays	3.5" Bays - QTY 4.
Raid Controller	512MB Controller with WIAP.
Raid Level Supported	RAID 0,1,5,6,10.
Input Power	100-240V.
BTU/HR	1194.
Power Supply	450 Watt - QTY 2.
Warranty	Five-Year Onsite.
Height	1.7".
Width	17.1".
Depth	29.5".
Weight (Max)	29 lbs.

Refer to Appendix E: Datasheets, "HNL-60126 06.00-26- 4C057 BCDVideo BCD104-170-MP-C.pdf."

2.2.23 Rack Mount DC Power Supply - AlarmSaf RM-PS5-MD-UL

The AlarmSaf Rack Mount DC Power Supplies fit standard IT equipment racks. They supply regulated and filtered main, standby, or auxiliary power for Access Control, CCTV, Fire, and Security systems integration applications. Models are available with fuse protected or power limited outputs and/or fire alarm interface capability if required.

Features

- Dual Power supply in a single Rack Mount enclosure
- 12 or 24 VDC, user selectable
- Fire Alarm Interface Capability on selected models
- Thermal protection
- Visual fault indication and reporting

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 62 of 430

- Overcurrent protection
- Battery presence supervision with optional disable
- Earth ground fault detection with optional disable
- Reverse battery protection
- Controlled current battery charging
- Illuminated master power switch with circuit breaker
- Input and output surge suppression
- Standard, 2U EIA 19" rack mount chassis
- Removable faceplate
- Removable terminal strips for field wiring
- Removable 3-wire grounded AC line cord
- Optional hardwire capability
- Limited lifetime warranty



Figure 33. Rack Mount DC Power Supply - AlarmSaf RM-PS5-MD-UL

[Table 24](#) provides the specifications for the rack mount DC power supply.

Table 24. Rack Mount DC Power Supply - AlarmSaf RM-PS5-MD-UL

Specifications	Description
Input Specifications	Input voltage: 120 VAC Input voltage frequency: 50 or 60 Hz Input Current: 2.5 A maximum
Output Specifications	Output voltage: 12 or 24 VDC, user selectable Output power: - 200 Watts total - Single Voltage Mode: 16A @ 12 VDC or 8A @ 24 VDC - Dual Voltage Mode: 8A @ 12 VDC and 4A @ 24 VDC Fuse Ratings - Battery: 15 A - FAI Main Output: 10 A Full load ripple: 0.015V p-p typical, 0.04V p-p during battery charge Electronically regulated and filtered output
Fire Alarm Interface (FAI) Specifications*	One main FAI output Control Input Voltage: 9 -33 VDC Control Input Current: 3.3 mA maximum

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 63 of 430

Table 24. Rack Mount DC Power Supply - AlarmSaf RM-PS5-MD-UL

Specifications	Description
	Dry contact input Open collector input
Temperature Ratings	Operating Temperature : 0° C to 49° C Humidity : 95% @ 32° C BTU/hr: 160 BTU maximum
Battery Charger Specifications	2 independent charger outputs - Battery Type: Sealed lead-acid rechargeable - Maximum battery charge capacity 80 Ah per charger - Maximum battery charge current: 2 A
Fault Detection	- Loss of AC or brownout - Power supply output > ±10% - Over-temperature condition - Low battery voltage - Earth ground fault (user option) - Blown battery or AC fuse - No battery present (user option)
Fault Reporting	- Form 'C' relay contacts - AC Fault: Contact rating, 28 VDC @ 1 A - Common Fault: Contact rating, 28 VDC @ 1 A
External Visual Indicators	AC presence: Illuminated AC switch
Internal Visual Indicators	- AC presence: Green LED - AC fault: Yellow LED - Common fault: Yellow LED - Earth ground fault: Yellow LED - FAI active: Red LED
Mechanical	2U Rackmount chassis: 3.25" H x 19" W x 10" D 16 gauge painted steel

Refer to Appendix E: Datasheets, "HNL-60126 06.00-32- 4C044 AlarmSaf RM-PS5-MD-UL.pdf".

2.2.24 Surface Mount Magnetic Contact - GE 2507A

The 2500 Series is designed to be installed in commercial and industrial environments where a rugged sealed unit is required. It is ideal for metal doors, overhead doors, fences, and gates. Each model features a high strength extruded aluminum housing and is completely encapsulated in our exclusive polyurethane potting compound. The 2500 series feature wide gap distances and several models to meet any application need. Jacketed lead or armored cable is available.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 64 of 430



Figure 34. Surface Mount Magnetic Contact - GE 2507A

[Table 25](#) provides specifications for the magnetic contacts.

Table 25. Surface Mount Magnetic Contact - GE 2507A

Specifications	Description
Form A (2505, 2505A)	
Voltage	100V AC/DC max.
Current	0.5A max.
Power	7.5W max.
European Union Specification	48V AC/DC max.
Form C (2507, 2507A, 2507AD, 2507AH)	
Voltage	30V AC/DC max.
Current	0.25A max.
Power	3.0W max.
SPDT Lead Colors	
Black	Common
White	Closed Loop (N.O.)
Red	Open Loop (N.C.)
Listing	C-UL-US, UL-634

Refer to Appendix E: Datasheets, “HNL-60126 06.00-28-4C039 GE 2507A.pdf.”

2.2.25 Surface Mount Magnetic Contact - GE 2507AD

The Surface Mount Magnetic Contact - GE 2507AD is an industrial Wide Gap Surface Mount Magnetic Contact. The 2500 Series is designed to be installed in commercial and industrial environments where a rugged sealed unit is required. It is ideal for metal doors, overhead doors, fences, and gates. Each model features a high strength extruded aluminum housing and is completely encapsulated in polyurethane potting compound. The 2500 series feature wide gap distances and several models to meet any application need. Jacketed lead or armored cable is available.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 65 of 430

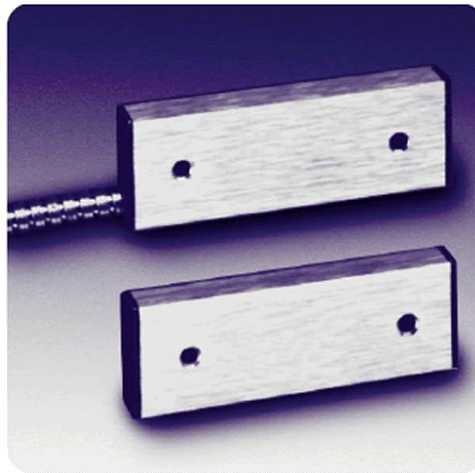


Figure 35. Surface Mount Magnetic Contact - GE 2507AD

[Table 26](#) provides specifications for the magnetic contacts.

Table 26. Surface Mount Magnetic Contact - GE 2507AD

Specifications	Description
Form A (2505, 2505A)	
Voltage	100V AC/DC max.
Current	0.5A max.
Power	7.5W max.
European Union Specification	48V AC/DC max.
Form C (2507, 2507A, 2507AD, 2507AH)	
Voltage	30V AC/DC max.
Current	0.25A max.
Power	3.0W max.
SPDT Lead Colors	
Black	Common
White	Closed Loop (N.O.).
Red	Open Loop (N.C.).
Listing	C-UL-US, UL-634.

Refer to Appendix E: Datasheets, “HNL-60126 06.00-28- 4C039 GE 2507AD.pdf.

2.2.26 Digital Loop Protector - EPS 3416D

Engineered Parking Systems (EPS).

Features:

- Automatic sensitivity boost – DIP switch selectable
- 10 sensitivity levels – rotary switch selectable
- Detector automatically tracks and compensates for environmental changes

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 66 of 430

- Loop failure indicator – green LED blinks indicating loop problem
- Loop failure memory – fast blinking green LED indicates past loop problem that healed
- 10-pin MS connector
- Loop input is transformer isolated
- Operating temperature range of – 40F to +180F
- Surge protection – neon discharge lamps, zener diodes, and surge arrestors
- Output relays rated 5 amps/125VAC
- Large loop inductance range: 20 to 2000 microhenries with Q factor of 5 or higher
- Three-position toggle switch for frequency selection
- Presence time – DIP switch selectable for infinite or 4 minutes
- Output can be extended for 3, 6 and 9 seconds
- Fail-Safe / Fail Secure – DIP switch selectable
- Pulse on entry/pulse on exit
- Extruded aluminum housing
- Height 3.25” – Width 2.56” – Depth 3.65”
- 110V AC Operation. Other voltages available

Refer to Appendix E: Datasheets, “HNL-60126 06.00-29- 4C040 EPS 3416D.pdf.”



Figure 36. Digital Loop Protector - EPS 3416D

2.2.27 Preformed Vehicle Detection Loop - EPS PFL46

The PFL preformed vehicle detection loop is constructed of stranded wire conductors with XLP thermoplastic elastomer insulation jacketing. The outer shell is flexible nonmetallic 0.26” tubing. The vehicle detection loop includes electronic lightning protection. The lead-in wire is twisted, shielded, and 50 ft. long.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 67 of 430



Figure 37. Digital Loop Protector - EPS 3416D

[Table 27](#) provides specifications for the magnetic contacts.

Table 27. Digital Loop Protector EPS 3416D Specifications

Features and Specifications
Rugged and flexible TPE tubing with overall diameter of 0.26 inches suitable for saw-cut, tar, and concrete installation.
Lightning protection. Includes electronic lightning protection of vehicle detectors.
Comes with 50 ft. of twisted and jacketed lead-in wire.
Operating Temperature: -60° to +260°F.
Overall Diameter of loop wire: 0.26" tubing Loop dimensions: 4' X 8' standard (PFL-48), other sizes available. Call for special sizes. Lead-in wire: 50 ft. long, twisted wire in PVC jacket.

Refer to Appendix E: Datasheets, "HNL-60126 06.00-30- 4C041 EPS PFL46.pdf."

2.2.28 Pedestal - CEO 72-9C-D and LANDO-KY-20x14E

A dual height pedestal with one extension at 72" and the other at 42". It accommodates ADA-compliant specifications as well as car, SUV, and truck/bus applications. It's made with a larger, heavier gauge 8" x 8" baseplate but contains the same 4" x 4" universal faceplates as the 42-9C. It contains conduit access through its baseplate for electrical wiring up each post.



Figure 38. Pedestal - CEO 72-9C-D and LANDO-KY-20x14E

[Table 28](#) provides the specifications for the pedestal.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 68 of 430	

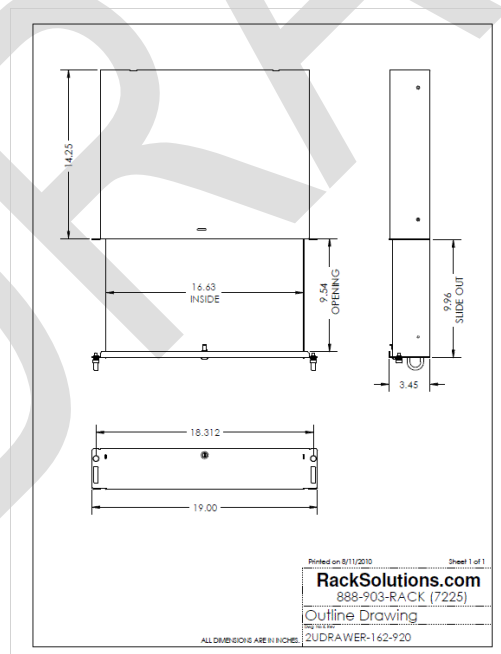
Table 28. Pedestal - CEO 72-9C-D and LANDO-KY-20x14E

Specifications	Description
Height	72" and 42".
Finish	Black Wrinkle TGIC Polyester Powdercoat - with UV Protectant.
Faceplate	4" x 4" Universal, .136 CRS.
Baseplate	8" x 8" Universal, .25 CRS.
Tube	2" x 4" Rec., .120 Wall (11 Gauge).
Neck	13", 90° Bend.
Material	Heavy Gauge Steel.
Box Size	45 lbs - Box Size: 76 x 15 x 11.
Hardware	Included: Carriage Bolts & Nuts.
Color Options	Black, Gold, White.
Customization Options	Custom heights and colors available.

Refer to Appendix E: Datasheets, "HNL-60126 06.00-31- 4C042 PedestalCEO 72-9C-D & LANDO-KY-20x14E.pdf."

2.2.29 Lockable Drawer - Rack Solutions 2U 162-920

A lockable drawer from Rack Solutions stores networking tools, patch cables, and manuals. All dimensions are in inches. Refer to Appendix E: Datasheets, "HNL-60126 06.00-35- 4C059 2U Lockable Drawer-162-920.pdf."


Figure 39. Pedestal - CEO 72-9C-D and LANDO-KY-20x14E

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 69 of 430

2.2.30 Glass Break Detector - Honeywell FlexGuard FG-730

The Honeywell FlexGuard® FG-730 incorporates a reliable, proven technology, setting an industry-standard in glass break detectors.



Figure 40. Honeywell FG-730

[Table 29](#) provides the specifications for the glass break detector

Table 29. Honeywell FG-730 Glass Break Detector Features

Features	Description
Dual Technology Flex-Audio Principle	Positively detects and confirms breaking glass by analyzing both “flex” (impact) and “audio” (shattering) frequencies. For an alarm to occur, the flex signal must be followed by an audio signal within a prescribed time frame.
Signal Verification	Both flex and audio signals must register valid amplitude, duration, and frequency for an alarm to occur.
Signal Filtering	Thorough filtering and processing of all signals provide greater immunity to false alarms.
Broad Range	Detects glass breakage from distances up to 30' (9 m). The FlexGuard FG-730 detector sets the industry standard in glass break detectors.
Dual Flex/Audio Technology	Provides excellent catch performance while virtually eliminating false alarms.
Indicator LEDs	LED alarm indicator for testing flex and audio technologies.
Burst Rejection Circuit	Ignores short flex/audio noise burst signals present in some environments.
Circuit Protection	Prevents shorts, overloads, and reverse-polarity connections from causing damage.
Alarm Memory	Alarm LED can be set to latch upon alarm; helps identify which unit alarmed in multiple detector applications.
RFI Immunity	100 watts at 3m (10') from all mobile bands 27–1000 MHz.
Low Voltage Operation	10–14VDC.
Low Current Draw	25mA at 12VDC.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 70 of 430

2.2.31 Instrumentation Cable - Exane Firewall LSZH Type TC

The Firewall® LSZH is totally low smoke, zero halogen cable comprised of both thermoset insulation and jacket material. It provides superior resistance to fire and moisture. It may be installed in wet and dry locations, indoors and outdoors, in metal trays, conduits, or ducts.

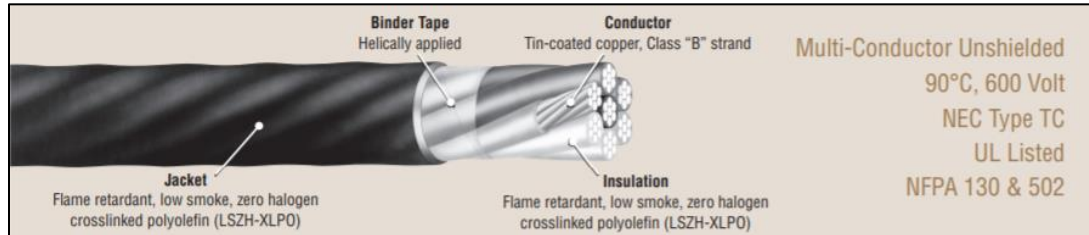


Figure 41. Exane Firewall LSZH Type TC

Table 30 provides the specifications for the Exane Firewall cable.

Table 30. Exane Firewall KSZH Type TC Specifications

Features	Performance Standards	Construction
Low Smoke Zero Halogen Design	Insulation in accordance with ICEA and UL standards	Conductor: Annealed, tin-coated copper, class "B" strand (ASTM B-8 & B-33).
RoHS compliant insulation and jacket	Insulated conductors are UL Listed Type RFHH-2	Insulation: Flame retardant low Smoke Zero Halogen crosslinked polyolefin.
Thermoset insulation for enhanced thermal stability	UL listed type TC (UL 1277) in accordance with NEC	Circuit Identification: Printed numbers per ICEA Method 4. (Alt. colors available upon request).
Specially formulated insulation for exceptional long-term water resistance	Passes IEEE 1202/FT4 vertical tray flame test and ICEA 70,000 BTU/hr vertical tray flame test (T-30-520)	Fillers: (Where required).
Superior flame retardance	Single conductors pass vertical flame test Type A as defined in ICEA S-95-658 (6.8.2)	Binder tape: Helically applied polyester.
Excellent mechanical properties	UL listed Type LS (limited smoke) per UL 1277 and UL 1685	Jacket: Reduced wall, black, flame retardant cross-linked low smoke zero halogen polyolefin.
Tin-coated copper conductors for improved terminations and corrosion resistance	UL approved 90°C for both wet and dry locations.	
Reduced size and weight for increased raceway capacity	Jacket exceeds requirements for UL class XL/90°C and ICEA publication T-33-655, Type II.	
Easy strippability	UL listed for sunlight resistance.	

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 71 of 430

Table 30. Exane Firewall KSZH Type TC Specifications

Features	Performance Standards	Construction
Low friction jacket for reduced pulling tension.	UL listed as gasoline and oil resistance.	
	Meets the requirements of NFPA 130 & 502.	

2.3 ACS FIELD COMPONENTS

Because the components of the ACS and IDS are deployed throughout the entire HART system, all field devices are described in the sections below, regardless of location.

2.3.1 ACS/IDS Panel

The ACS/IDS includes field panels with integrated controllers to process and manage all alarm inputs and card reader devices deployed at a specific location. These controllers (installed in field panels) are deployed at station TCCRs, MSF buildings, and TPSS locations. These controllers are the integration point between the field devices and the central server. Each controller is connected to the SLAN, which provides transmission support for data to and from the server.

The controller includes integrated storage of credential authorizations allowing it to function independently of the centralized server for extended durations. This functionality increases the reliability of the system and reduces the potential for user lock-outs in the event of transmission or central server failure.

The ACS/IDS controller receives requests for access and alarm imitation at project sites such as MSF facilities and stations. When requested, the ACS provides access to areas via a locally stored database for the specific field location and communicates alarms to the CCTV system to provide event-driven video on any client workstation with connectivity to the CTS and SLAN networks.

The ACS/IDS controller is a separate and individual printed circuit board of the same manufacture as all other equipment in the ACS/IDS. Panels for this function have no less than the following minimum requirements:

- Operate on 12/24 VDC
- Provide one NIC port for IP communications with the ACS server.
- RS 485 communications ports for local device communications

2.3.2 ACS/IDS Input Boards

ACS/IDS Input Boards are installed along with and connected to the ACS/IDS panel and provide a point of connection for all dry contact monitor points on the system.

ACS/IDS Input Boards communicate to the ACS/IDS panel and connect to field monitor points sending signals to the ACS/IDS Controller to report a change in state of a monitored point. These panels also provide five-state supervision of the device and cabling to report changes or faults in the wiring and device.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 72 of 430

2.3.3 ACS/IDS Output Boards

ACS/IDS output boards are installed with and connected to the ACS/IDS panel and provide a point of connection for all controlled points on the system. ACS/IDS output boards communicate to the ACS/IDS panel and connect to field controllable points upon receipt of signals to the ACS/IDS control panel to control a change in the state of a filed point. These panels also provide five-state supervision of the device and cabling to report changes or faults in the wiring and device.

2.3.4 ACS/IDS Door Interface

The ACS/IDS door interface is installed at each controlled door, gate, or other hardware. The interface communicates with the ACS/IDS panel while receiving signals from the card reader at the point of access.

ACS/IDS door interface communicates to the ACS/IDS panel and connects to field controllable points and card readers at the control locations. Upon receipt of authorized information from the readers, the interface communicates with the ACS/IDS panel to control peripheral devices that authorize entry. These panels also provide five-state supervision of the device and cabling to report changes or faults in the wiring and device. It accepts the dry connections from door/gate devices and provides supervision of each for faults and troubles. The unit also controls door unlocking via a dry contact with switched power from system power supplies to hardware installed at the opening. Finally, the interface receives and processes data from the attached card readers and provides authorization when a valid credential is presented.

2.3.5 ACS/IDS Card Reader

The ACS/IDS card reader is installed at each controlled door and processes information from employee badges for controlled access. It communicates to the ACS/IDS door interface by reading information on cards coded with the unique client and individual information.

The ACS/IDS card reader decodes information on employee badges and communicates that information to the ACS/IDS door interface. Badges of like-kind or technology may be recognized on the system - but without a site and user-specific information and authorizations, they will be invalid.

2.3.6 Intrusion Alarm Sensors (Contacts)

Alarm contacts are distributed throughout the system and provide information on opening and cabinet door states of equipped devices. These contacts are present on Automated Electronic Defibrillators (AED), equipment cabinets, restricted access doors, gates, and other locations that require remote intrusion alarming.

Alarm contacts provide the status of the door and cabinet position via an internal switch affected by a corresponding magnet. The alarm contact monitors door and cabinet position and provides a signal to the access control system upon a change in state. Devices have five-state supervision to detect device and wiring faults or tampering.

2.3.7 Traffic Loop Detector

A traffic loop is installed at the main gate to the MSF secured area. A detector is installed on both sides of the gate on the inside (secure) side of the gatehouse. The loop is designed to provide an automated signal to the gate arm to open when a vehicle leaves the secure area.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 73 of 430

The loop is a continuous run of wire that enters and exits from the same point and is embedded in the road. The two ends of the loop wire are connected to the loop extension cable, which in turn connects to the vehicle detector. The detector powers the loop causing a magnetic field in the loop area. The loop resonates at a constant frequency that the detector monitors. A base frequency is established when there is no vehicle over the loop. When a large metal object, such as a vehicle, moves over the loop, the frequency increases and resonates. This increase in frequency is sensed and forces a normally open relay to close. This loop close event triggers the gate to open or the gate arm to rise without manual intervention.

2.3.8 Intrusion Alarm Panel

At each station and each MSF building, an intrusion alarm panel is installed near the station fire alarm panel and at the OCC guard office. An Intrusion alarm panel is also installed within each TPSS. This panel has LED lights that illuminate what an area with an intrusion alarm sensor is opened (regardless of access authorization). This allows the ability to identify any open areas throughout the station, MSF, or TPSS from one location. If an intrusion alarm sensor is activated without proper authorization, the ACS/IDS panel initiates an audible alarm at the Intrusion Alarm Panel. The panel is reset remotely or by a physical key.

2.3.9 Intercom

At main entry areas in the MSF, specifically the main gate, Operations Service Building (OSB) front door, Maintenance of Way (MOW) front door, and the OCC entrance door, an intercom device is installed to provide the ability to communicate with an employee who can remotely unlock that door.

The intercom is an IP-based audio device connected via the SLAN to the network infrastructure. When the call button is depressed, a Voice Over IP (VOIP) call is placed using the system private automatic branch exchange (PABX) to a pre-defined number. When the call is connected, the call operates as a normal voice call. To remotely unlock the door for the caller, the call recipient dials "9" on the telephone keypad. A signal is generated from the PABX to the ACS server, which then sends a remote unlock signal to the door through the ACS/IDS system.

2.3.10 Knox Box

At each station, MSF building, and the MSF main gate, a Knox box is installed to allow first responder access to physical keys to access the facility. These boxes are not electronically connected to the ACS/IDS system but are alternative means for First responders to gain access to normally locked areas during an emergency.

2.4 ACS SOFTWARE - GENETEC SECURITY CENTER

Genetec *Security Center* software used with Synergis master for programming of the ACS. Omnicast is the previous brand name/version that reached its end of life (EOL) and has been replaced by Genetec with the brand name *Genetec Security Center*. Genetec Omnicast/*Security Center* is the IP video surveillance system that provides seamless management of digital video on top of the Security Desk platform.

Security Center lets you use multiple vendors and CODECs (coder/decoder) within the same installation, providing the maximum flexibility when selecting the appropriate hardware for each application. *Security Center's* main features include:

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 74 of 430

- View live and playback video from all cameras
- View up to 64 video streams side-by-side on a single workstation
- View all cameras on independent timelines or on synchronized timelines
- Full PTZ control, using a PC or CCTV keyboard, or on screen using the mouse
- Digital zoom on all cameras
- Motion detection on all cameras
- Visual tracking: follow individuals or moving objects across different cameras
- Search video by bookmark, motion, or date and time
- Export video
- Protect video against accidental deletion
- Protect video against tampering by using watermarks
- Provides video support for events tracked by other systems unified under Security Center.
- Enhance all event reporting with live and playback video
- Enhance alarm monitoring with live and playback video
- Enhance intrusion detection with live and playback video
- Enhance access control system (Synergis) with live and playback video
- Video verification: compare cardholder picture with live and playback video
- Consolidate all access events with live and playback video

2.4.1 Genetec Synergis

Synergis is the IP access control system of the *Security Center* that provides end-to-end IP connectivity, from access control reader to client workstation. It seamlessly integrates a variety of access control capabilities, including, but not limited to, badge design, zone monitoring, and more. It was designed with an open and distributed architecture, so it allows HART to integrate its access control system with other third-party systems, like intrusion or building management, and distribute Synergis server components on many different network machines to optimize bandwidth and workload.

Synergis Enterprise supports an unrestricted number of doors, controllers, and client workstations. You can grow your system one door at a time or scale your system across multiple buildings using the Federation feature. Synergis™ architecture is based on the server role known as the **Access Manager**, which controls the physical door controllers.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 75 of 430

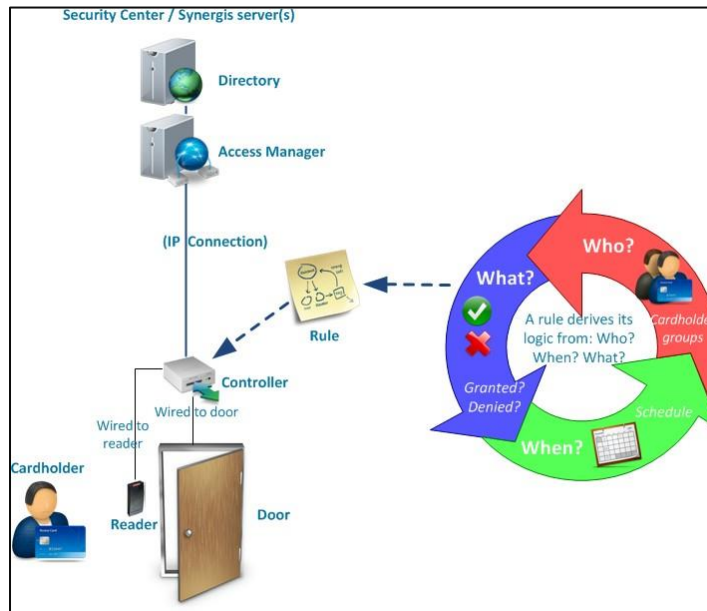


Figure 42. Synergis Architecture

The following provides a general description of how Synergis™ architecture works:

- System configurations are saved by the Directory role.
- The Directory pushes configurations to the Access Manager.
- Access Manager communicates directly with the physical door controllers, called access control units, over TCP/IP.
- Access Manager pushes schedules, cardholder information, and access rules to the door controllers.
- When a cardholder presents their credential to a reader, the controller refers to the access rule to determine whether the user should be granted or denied access.
- Once controllers have synchronized with the Access Manager, they can operate autonomously, even if they lose the network connection to the Access Manager.

With additional configuration, a cardholder can belong to a cardholder group, a door can be part of an area, and there can be multiple schedules and rules pushed to a unit.

2.4.1.1 How Access Events Display in Tiles

An **access event** (access granted, or access denied: invalid PIN, etc.) is any event involving an access point. When an access event occurs on an entity you are monitoring, information about the event is displayed in a tile in the Monitoring task.

Figure 43 is an example of an **Access Denied** event. The event description is displayed at the top of the tile as a colored overlay. Additional information, such as the event timestamp and the cardholder name is displayed when you place the cursor over the colored overlay. Also, you can expand the cardholder picture by placing the cursor over the picture. This might be helpful when comparing the cardholder picture to the face you see in the video.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 76 of 430	



Figure 43. Example of Access Denied Event

2.4.1.2 Antipassback

An antipassback violation occurs when a cardholder enters an area that they never exited or when they exit an area that they never entered. This can occur when an authorized cardholder unlocks a door, and while entering, passes their card back to somebody else.

The *Security Center* administrator can configure the system to deny access to that cardholder. When this happens, you must click the **Forgive antipassback violation** (👉) button to let the cardholder in or out. For information about applying antipassback to areas, see the *Security Center Administrator Guide*.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 77 of 430	

3 GENETEC SYNERGIS

Genetec Synergis is based on the complete *Genetec Security Desk* platform, which includes built-in functions for ACS and IDS and uses *Security Center* as the interface. HART operators learn how to use the basic functions of the *Security Desk* in the HNL-62706 ICCS Operations Manual.

3.1 SECURITY CENTER

Security Center is a unified platform that blends IP video surveillance, access control, intrusion detection, and communications within one intuitive and modular solution. By taking advantage of a unified approach to security, your organization becomes more efficient, makes better decisions, and responds to situations and threats with greater confidence.

The Security Center unified security platform provides the following advantages:

- One platform controlling and managing video/access edge devices.
- One user interface for monitoring, reporting, and managing events and alarms for video surveillance and access control - Security Desk.
- One user interface for configuring video surveillance and access control - **Config Tool**.
- Unified live video viewing with video searches and video playback.

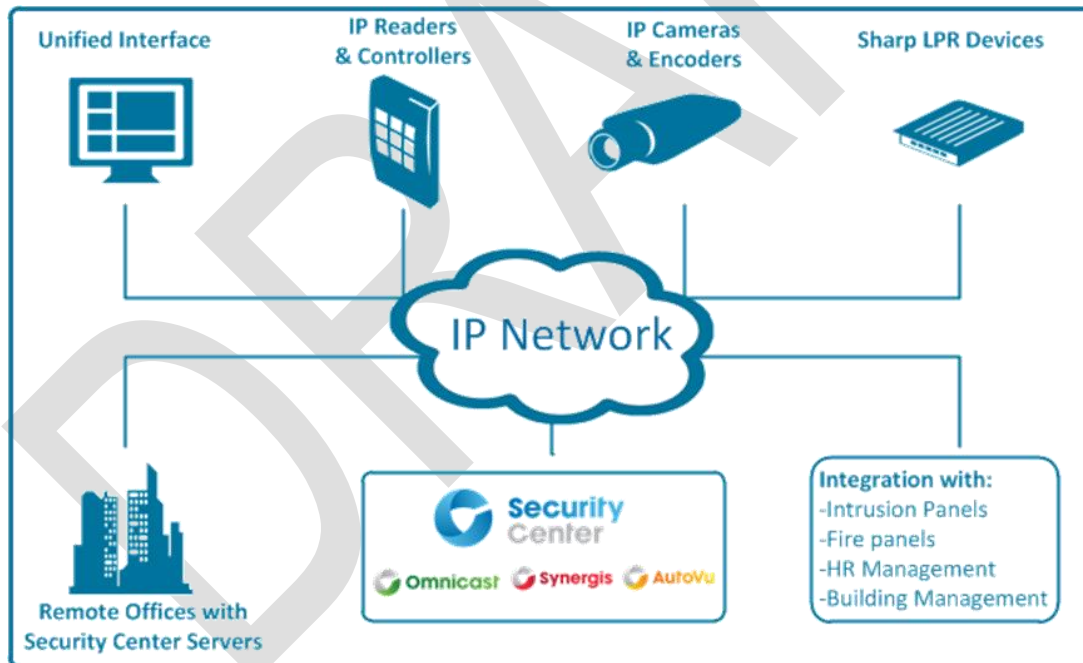


Figure 44. Security Center Access Control Integration

HART uses three main categories of Security Center applications: common, video surveillance (Omnicast), and access control (Synergis).

Common/Core Features

- Alarm management

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System Operations Manual		Page 78 of 430

- Zone management
- Federation
- Intrusion panel integration
- Report management
- Schedule and scheduled task management
- User and user group management
- Windows Active Directory integration
- Programmable automated system behavior

Omnicast – Video surveillance features

- Full camera configuration and management
- View live and playback video from all cameras
- Full PTZ control using the PC or CCTV keyboard, or on screen using the mouse
- Digital zoom
- Motion detection
- Bookmark any important scene to ease future video archive search and retrieval
- Save and print video snapshots
- Search video by alarm, bookmark, event, motion, or date and time
- View all cameras on independent or synchronized timelines
- Visual tracking: follow individuals or moving objects across different cameras
- Export video
- Protect video against accidental deletion
- Protect video against tampering by using watermarks
- Protect the privacy of individuals in the video

Synergis™ – Access control features

- Cardholder management
- Credential management
- Door management
- Access rule management
- People counting

Security Center Synergis™ is the IP ACS that heightens HART's physical security and increases HART's readiness to respond to threats. Supporting an ever-growing portfolio of third-party door control hardware and electronic locks, it allows HART to leverage existing investment in network and security equipment.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 79 of 430

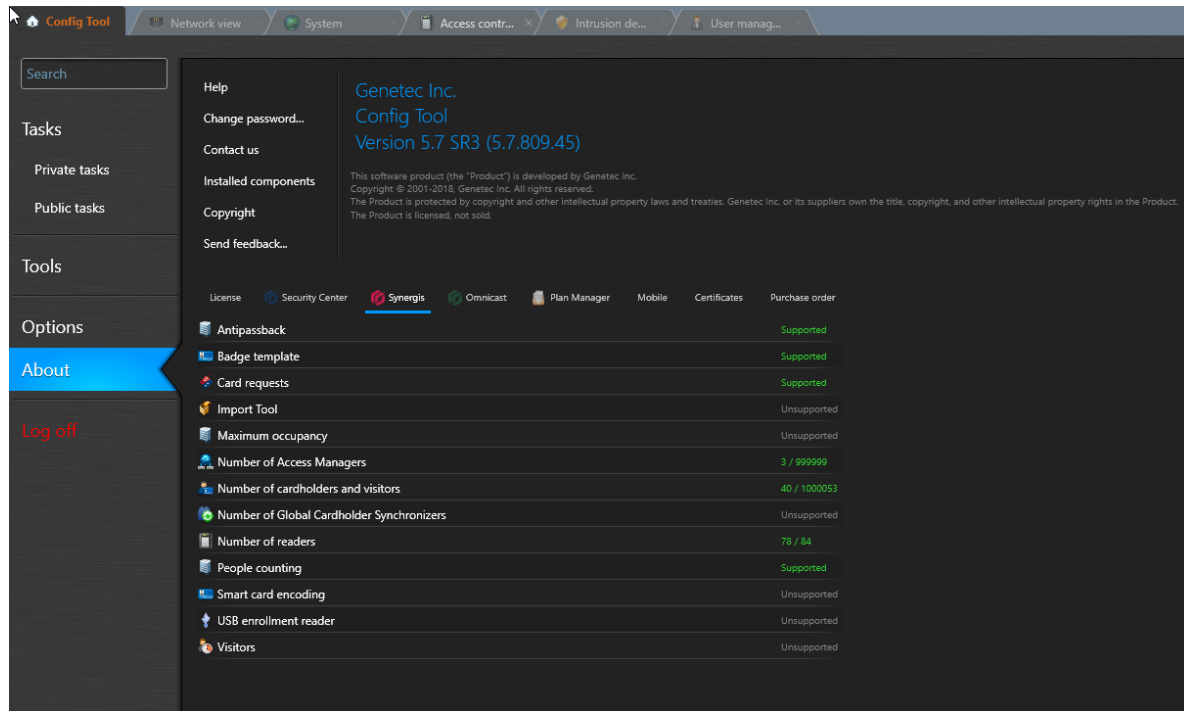


Figure 45. Genetec Synergis: About Config Tool: Version 5.7 SR3 (5.7.809.45)

3.1.1 Security Center Architecture

Security Center's architecture is based on a client/server model, where all system functions are handled by a pool of server computers distributed over an IP network.

Every *Security Center* system must have its own pool of servers. Their number can range from a single machine for a small system to hundreds of machines for a large-scale system.

- **NOTE:** The icons colored in blue represent the computers where the *Security Center* server and client components are installed.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 80 of 430

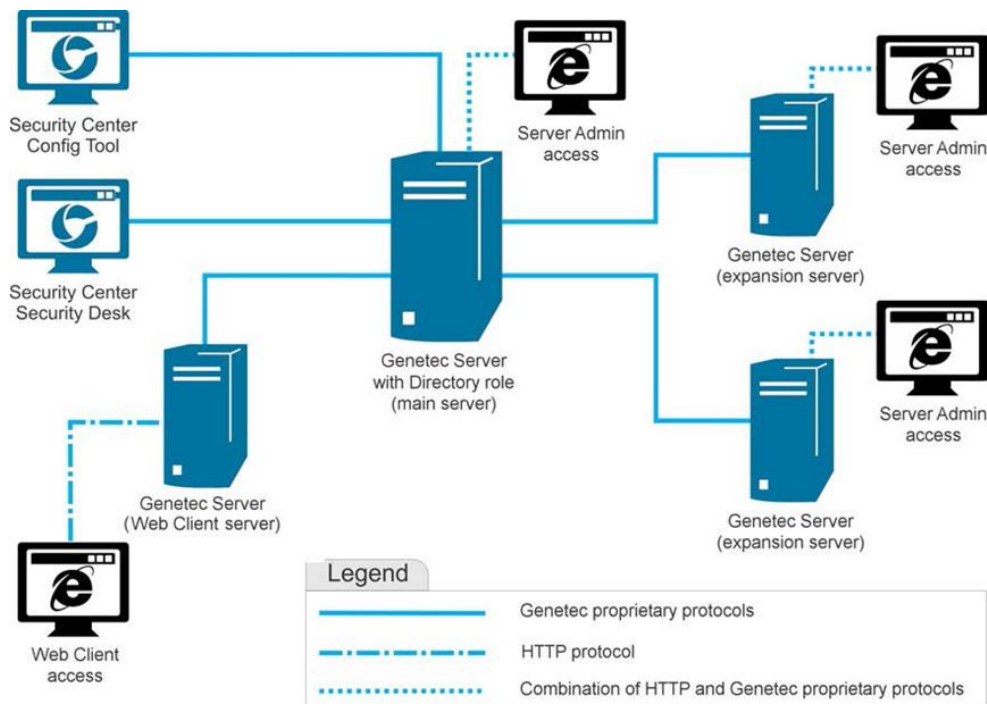


Figure 46. Security Center: Architecture

3.1.2 How the Security Center is Organized

Security Center is organized by tasks. All tasks can be customized, and multiple tasks can be carried out simultaneously. You might not see all the tasks and commands described about Security Center, depending on your license options and user privileges. There are user privileges for each task, and for many commands in Security Center.

Tasks in the home page are organized into the following categories:

- **Administration:** (Config Tool only) Tasks used to create and configure the entities required to model your system.
- **Operation:** Tasks related to day-to-day Security Center operations.
- **Investigation:** (Security Desk only) Tasks allowing you to query the Security Center database, and those of federated systems, for critical information.
- **Maintenance:** Tasks related to maintenance and troubleshooting.
- Under each major category, the tasks are further divided as follows:
 - **Common tasks:** Tasks that are shared by all three Security Center software modules. These tasks are always available regardless of which modules are supported by your software license.
 - **Access control:** Tasks related to access control. Access control tasks are displayed with a red line under their icons. They are only available if *Synergis™* is supported by your software license.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 81 of 430

- **Video:** Tasks related to video management. Video tasks are displayed with a green line under their icons. They are only available if Omnicast™ is supported by your software license.

3.2 INSTALLATION

This section briefly describes installation procedures.

3.2.1 Server Installation

For Genetec installation and administration guides, refer to [Appendix H. OEM User Manuals](#).

The following OEM user manuals are included

- Genetec Security Center Installation and Upgrade Guide 5.7 SR3
- Genetec Security Center Administrator Guide 5.7
- Genetec Security Center 5.7 System Requirements
- Genetec Security Center 5.7 Ordering Guide
- Genetec Security Desk User Guide 5.7
- Getting Started with Security Desk 5.7
- Security Center 5.7 Network Diagram - Access Control
- Security Center Best Practices 5.7 Access Control
- Genetec AC Train Mats-Part 3 Chap 14-19 Synergis Security Desk User Guide 5.2

3.2.2 Client Workstation Installation

To install the *Genetec Security Center* on a workstation:

1. Ensure that you have a valid IP address and that you can ping the server.
2. Navigate the contents of your USB flash drive to the path: **\\Security Center 5.x**
3. Right-click the file and select **Properties**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 82 of 430

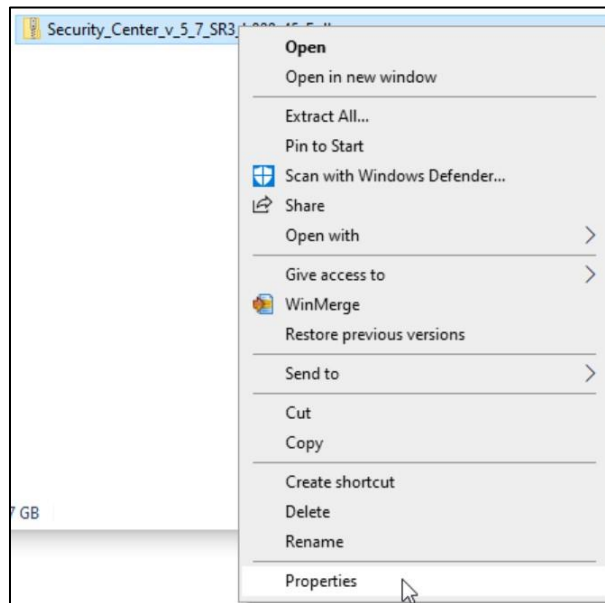


Figure 47. Security Center Workstation Installation: Right-Click File and Select Properties

4. On the **General** tab click the check box for **Unblock** and apply this to the file.

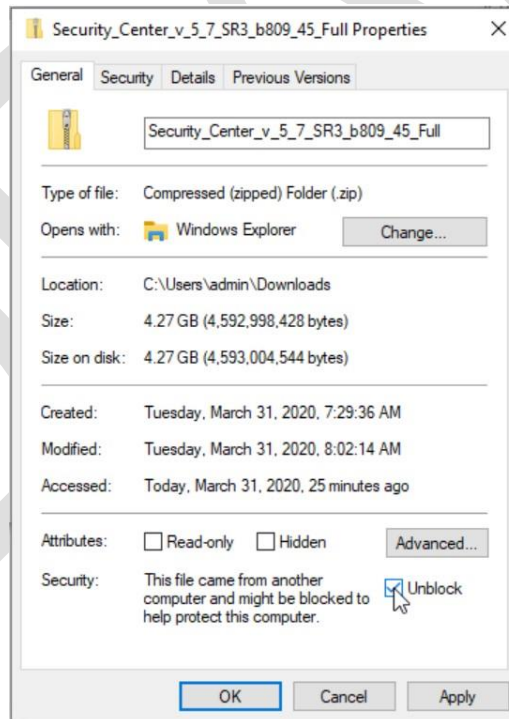


Figure 48. Security Center Workstation Installation: Unlock Security in General Tab

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 83 of 430

5. Now you can extract the files and proceed to run the installation.

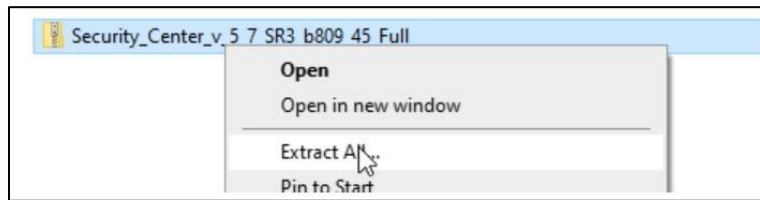


Figure 49. Security Center Workstation Installation: Select 'Extract All'

6. Right-click the file **setup.exe** and select **Run as administrator**.

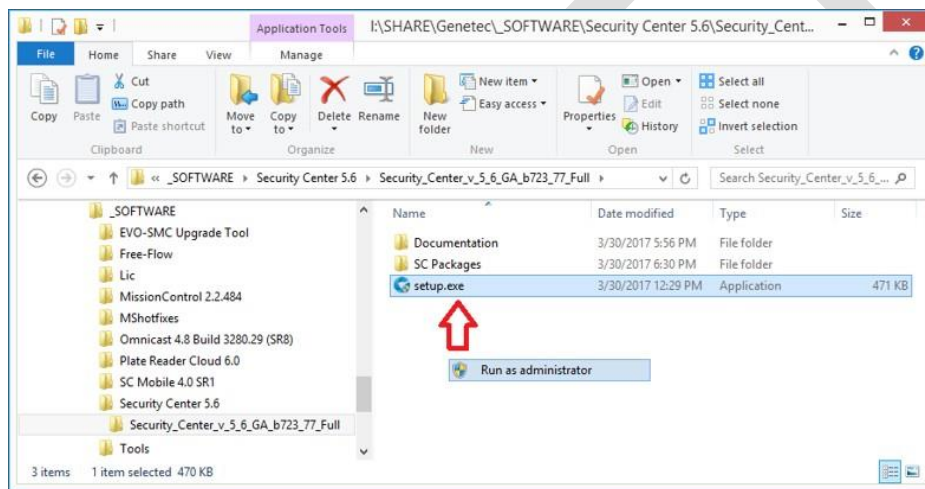


Figure 50. Security Center 5.x Client Installation: Setup.exe

7. Follow the **InstallShield wizard** to install the Security Center 5.x client software.
8. Allow the installer to install any prerequisite software (.NET, Visual C++, Windows hotfixes...) If the .NET framework must be installed, be patient, it takes some time.

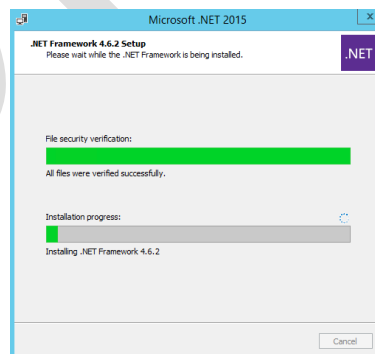


Figure 51. Security Center 5.x Client Installation: NET Framework

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 84 of 430

A reboot is required before continuing with the *Security Center* installation.

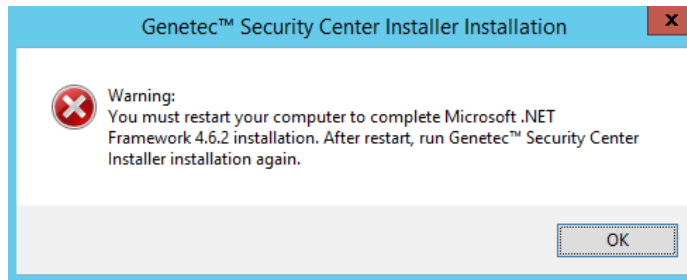


Figure 52. Security Center 5.x Client Installer

9. Once the installer is ready to install the Security Center 5.6 components, make sure that the Server is unselected and that only the Client is selected.

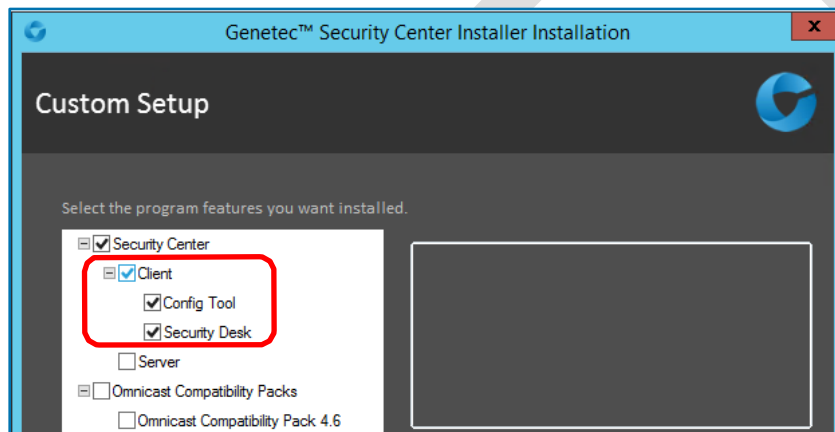


Figure 53. Security Center 5.x Client Installation: Custom Setup

10. When prompted, agree to participate in the collection of system usage information (Participate, or participate anonymously).

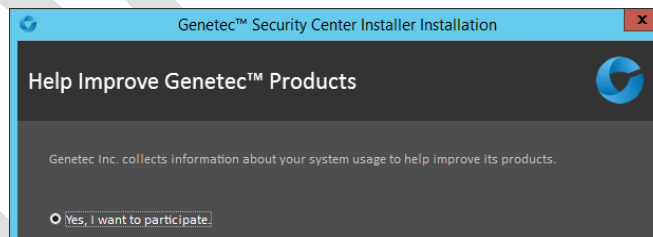


Figure 54. Security Center 5.x Client Installation: System Usage Participation

11. Allow **High-Performance** configuration of the firewall rules.
12. From the **Security Settings** page, select **Custom** (Advanced), then:
 - Always validate the **Directory** certificate.
 - Turn off basic authentication.
 - I acknowledge...

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 85 of 430

13. Follow the prompts to complete the client installation.

3.2.2.1 Test Client Installation

1. Test your client software by launching your **Config Tool** application.
2. Once the Main server installation is complete, try to connect to the server using:
 - **User:** Admin **Password:** (none)
 - **Directory:** Name or IP of the server.

3.2.2.2 Post-Installation (Video Benchmark Test)

The hardware benchmark tool enables you to calibrate your settings to optimize the performance of your installed video cards. You can run the hardware benchmark tool in Config Tool or Security Desk.

You are prompted to run the hardware benchmark tool the first time you start the Security Desk. There is also a yellow warning icon that appears on the notification tray whenever you change your video card configuration. There are no prompts in the **Config Tool**.

- Running the benchmark tool is GPU intensive. Close all other tasks and applications when performing a benchmark test to ensure you get valid results.
- For best results, make sure your GPU drivers are up to date before running the hardware benchmark tool.

To Use the Hardware Benchmark Tool:

1. In the notification tray, click the **Resources meter** icon (📊). The Hardware information dialog box opens. From the **Acceleration** dropdown list, select the video card you want to run the benchmark test on.
2. Click **Run benchmark**.
3. Once the benchmark test is complete, the Frame rate capability of the selected card is listed.
4. Click **Close**.

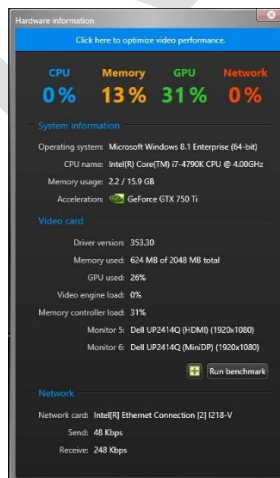


Figure 55. Genetec Security Desk – Hardware Benchmark Tool

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 86 of 430

3.3 QUICKSTART GUIDE

This section provides instructions to log on and off Security Center.

3.3.1 Log On

To log on, open the Security Desk application and connect to the Security Center server. Make sure you have your username, password, and the name of the Directory that you want to connect to. Once you are logged on, you can log off and disconnect from the Directory without closing Security Desk. Logging off without closing the application is helpful if you plan to log on again using a different username and password.

- **NOTE:** After a period of inactivity, you might be locked out of the Security Desk. You must enter your credentials to use the application again.

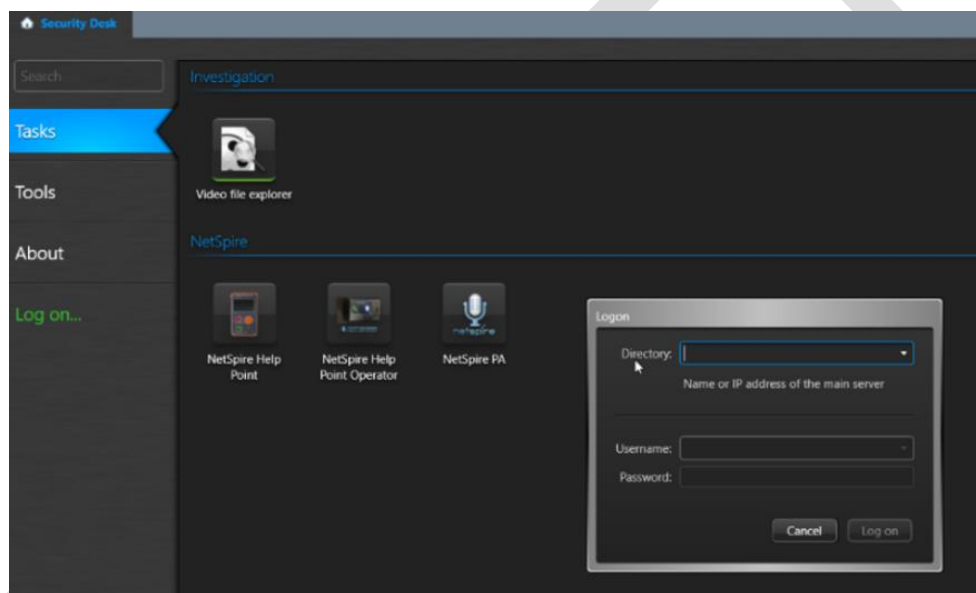


Figure 56. Security Desk - Log On Window

To Log On to Security Desk

To open Security Desk, click **Start > All programs > Genetec Security Center 5.7 > Security Desk**.

1. In the **Log on** dialog box, do one of the following:
 - Enter your *Security Center* username and password.
 - Log on using your **Windows** user account by selecting **Use Windows credentials**.
2. In the **Directory** field, enter the name or IP address of the main *Security Center* server.
3. If you are required to log on with supervision, your supervisor must provide a username and password.
4. Click **Log on**.

To **log off**, click the **Home** tab (🏠) and then click **Log off**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 87 of 430

3.3.1.1 Log On to Security Center Through Config Tool

To log on to *Security Center*, you must open the **Config Tool** and connect to the *Security Center* Directory. Make sure that you have your username, password, and the name of the main server that you want to connect to.

Logging on to *Security Center* typically involves a two-way authentication:

- The Directory (main server) must be authenticated by the party requesting the connection (the user).
- The party requesting the connection must be authenticated and authorized by the Directory.

Security Center offers different options to handle the authentication process. Your logon procedure might take on different paths, depending on how the administrator has set up your system.

After you are logged on, you can disconnect from the Directory without closing **Config Tool**. Logging off without closing the application is helpful if you plan to log on again using a different username and password.

To log on to *Security Center*:

1. Open **Config Tool** by clicking **Start > All Programs > Genetec Security Center 5.7 > Config Tool**.
2. In the **Logon** dialog box, enter the name or the IP address of your main server as Directory.

NOTE: If you are running **Config Tool** on the main server, you can enter *Localhost* instead of the main server name.

If the Directory is not responding, make sure the server is online and that your network configuration allows your computer to contact the main server (check hostname, IP address, and firewall rules).

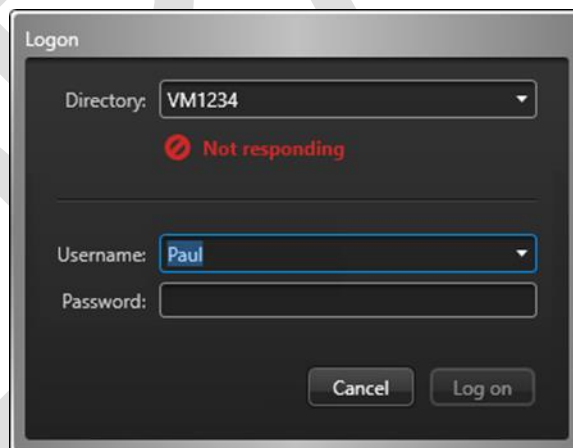


Figure 57. Log On

If the Directory is not trusted, it could be the sign of a man-in-the-middle attack. Do not proceed unless you (or your administrator) are certain that the server you are contacting is secure.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 88 of 430

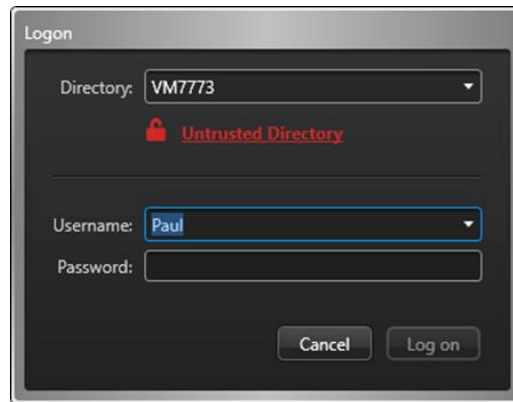


Figure 58. Log on: Untrusted Directory

Click the **padlock** icon for more information.

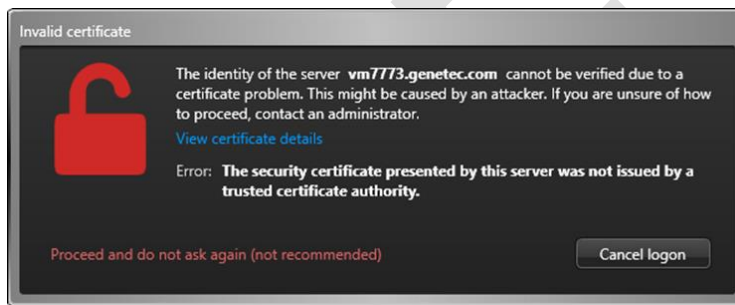


Figure 59. Log On: Invalid Certificate

If your administrator confirms that you can trust that server, click **Proceed** and do not ask again. The certificate of that machine will be stored on your machine, and future connections to that same Directory will be trusted, as long as its certificate does not change.

3. Enter your *Security Center* username and password.

If you have just installed *Security Center*, enter *Admin* with a *blank* password.

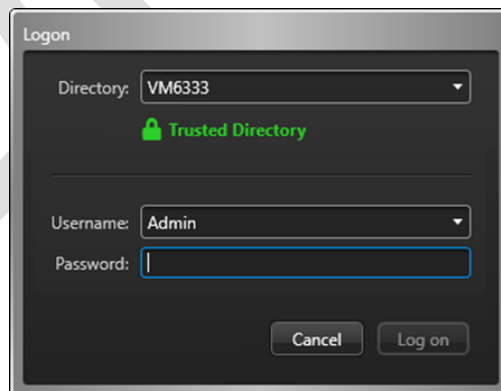


Figure 60. Log On: Trusted Directory

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 89 of 430	

If single sign-on (Active Directory or ADFS) is deployed, you must append your domain name to your username, such as in *Username@DomainName*.

If *Security Center* detects that passive authentication with ADFS is enabled on your domain, you will be redirected to a web form displayed by the identity provider after you have entered your username. Skip to [Log On Using Passive](#) Authentication.

4. To log on using your **Windows** user account, select Use **Windows** credentials. This option is only available if Active Directory is set up on your system.

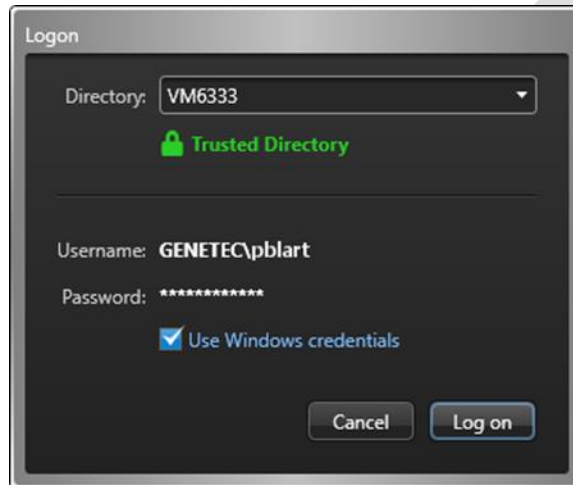


Figure 61. Log On: Windows Credentials

- **NOTE:** If your client workstation is not on the same domain as your server, or if you want to log on to *Security Center* with a different Windows account, you must clear the **Use Windows credentials** option and type your username in the format DOMAIN\Username.

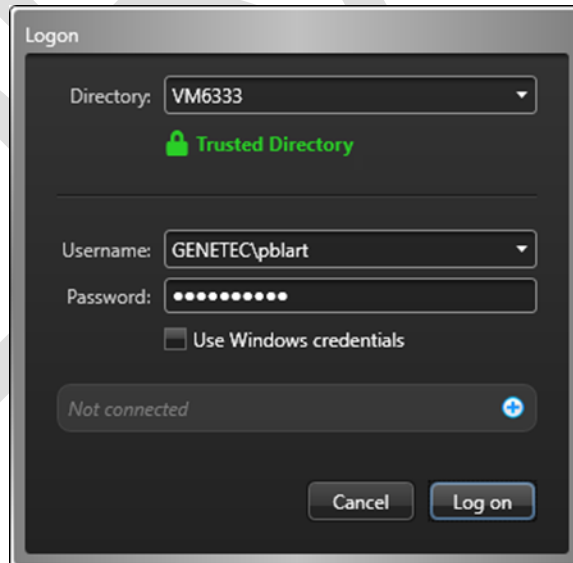


Figure 62. Log On: Clear Windows Credentials: DOMAIN\Username

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 90 of 430

5. Click **Log on**.
6. To log off, click the **home** (🏠) tab, and then click **Log off**.

3.3.1.2 Log On Using Passive Authentication

If *Security Center* detects that your logon username matches the domain covered by an ADFS server with passive authentication enabled, you will be redirected to a web form to enter your password.

Open **Config Tool** and enter the name of the Directory in the **Logon** dialog box.

Passive authentication (also known as web-based authentication) is when the client application redirects the user to a web form managed by a trusted identity provider. The identity provider can request any number of credentials (passwords, security tokens, biometric verifications, and so on) to create a multi-layer defense against unauthorized access. This is also known as multi-factor authentication.

- **NOTE:** **Config Tool** remembers all valid login parameters used and automatically calls up the parameters used for the last login attempt.

To log on using passive authentication:

1. In the **Username** field, enter your username, followed by your domain name, in the format *Username@DomainName*.

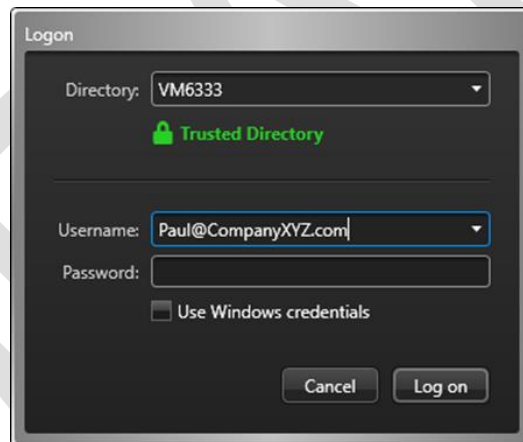


Figure 63. Passive Authentication Log On

2. Click the **Password** field or press the **Tab** key.

If *Security Center* detects that passive authentication is enabled on your domain, you will be redirected to a web form. The following figure is an example. Your **logon** page might look different.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 91 of 430

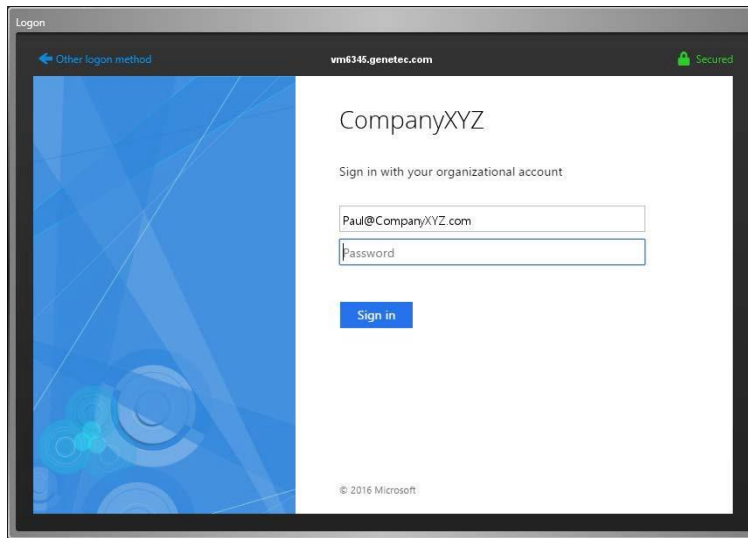


Figure 64. Log On: Webform

5. In the webform, enter the information that is required and click **Sign in**.
 - **NOTE:** You cannot log on as the **Admin** user using web-based authentication. To log on as the Admin user, click **Other logon** method to go back to the **Security Center Login** dialog.

3.3.2 Log Off

You can close and save your workspace for the next time you log on. By default, you are asked to save your workspace when you close the *Security Desk*. You can change this behavior from the **Options** dialog box.

To Log off and Close:

- In the upper-right corner of the Security Desk window, click the **Exit** button (). If you have unsaved tasks in your workspace, you are prompted to save them.
- To automatically load the same task, list the next time you open *Security Desk*, click **Save**.

3.4 SYSTEM ROLES

The following roles are installed by default with the current deployment of Genetec Synergis:

- [Directory Role](#)
- [Archiver Role](#)
- [Access Manager Role](#)
- [Media Router Role](#)
- [Zone Manager Role](#)
- [Report Manager Role](#)
- [Health Monitor Role](#)
- [Map Manager Role](#)

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 92 of 430

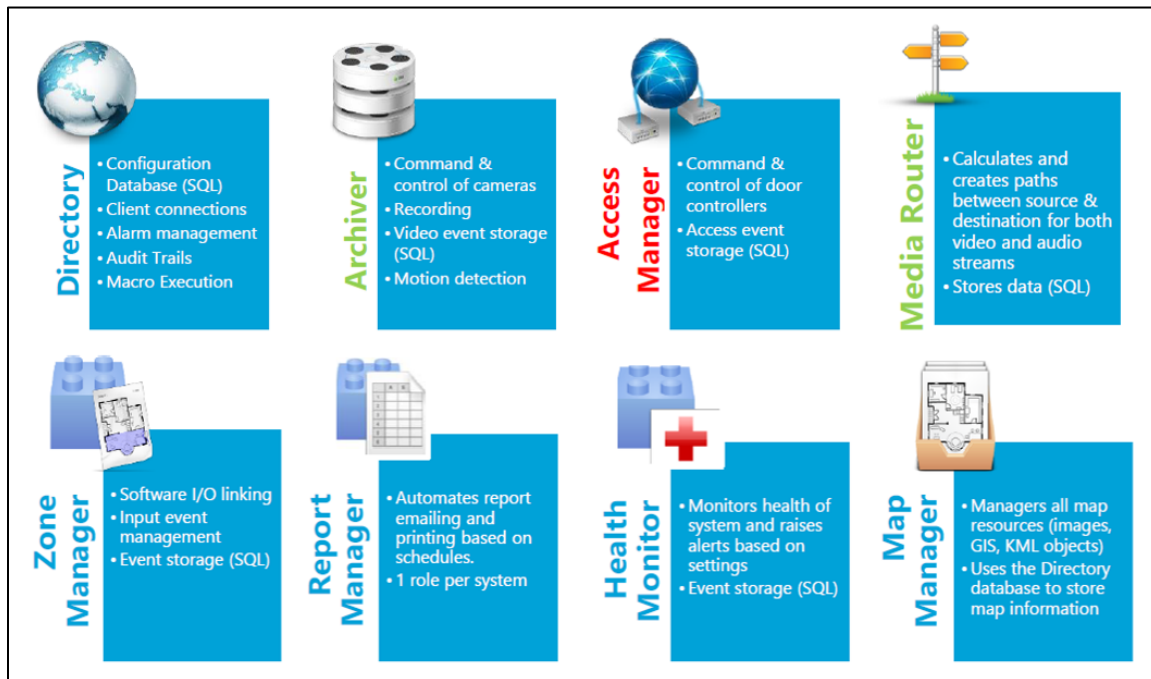


Figure 65. Security Center 5.7 Basic Roles

For a *Security Center* access system, the minimum server roles required are:

1. **Directory** - For client connections and system configuration db.
2. **Access manager** - For command and control of access control units, and logging of access events in the event db.

A role is a software component that performs a specific job within the *Security Center*. To execute a role, you must assign one or more servers to host it. You can assign roles for archiving video, for controlling a group of units, for synchronizing *Security Center* users with your corporate directory service, and so on. In the *Security Center*, role entities are defined by the following:

- **Role type**: Determines the specific set of functions that should be performed by the role, such as managing video units and associated video archives.
- **Role settings**: Define the specific set of parameters the role should operate within, such as the retention period for the collected data, or which database the system should use.
- **Servers**: The servers that should be hosting (running) this role.

You can assign one or more roles to the same server or assign multiple servers to the same role to provide load balancing and failover. After a role is configured, you can move it to any server in your *Security Center* system (for example, one with a faster processor or more disk space) without having to install any additional software on that server. Moving a role to another server might cause a short pause in the role's operations. In addition, some roles can spawn subprocesses (called agents) and execute them simultaneously on multiple servers for greater scalability.

3.4.1 Directory Role

Directory is the main role that identifies your system. It manages all entity configurations and system

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 93 of 430

wide settings. Only a single instance of this role is permitted on your system. The server hosting the Directory role is called the main server and must be set up first. All other servers you add in *Security Center* are called expansion servers and must connect to the main server to be part of the same system.

The main functions of the **Directory role** are:

- Client application connection authentication
- Software license enforcement
- Central configuration management
- Event management and routing
- Audit trail and activity trail management
- Alarm management and routing
- Incident management
- Scheduled task execution
- Macro execution

3.4.1.1 How Video Displays When the Directory Role Disconnects

The *Security Center Directory* role manages your entire system and without it you cannot log on to the system. If the server's Directory role is disconnected from the rest of the system, *Security Desk* starts to operate in a degraded mode.

If you were viewing a camera, you remain connected to that camera's live video stream even after you are logged out of the system. You can also view playback video if the live video was cached to your local workstation. The cached video is indicated by the orange bar at the top of the timeline.



Figure 66. Directory Role Disconnect: Video Cache

Security Desk constantly attempts to reconnect to the Directory. Once reconnected, the operating mode reverts to normal. [Figure 67](#) shows what the degraded mode looks like after a Directory failure; the letters correspond to the letter in the figure.

- The connection state icon shows that you are disconnected.
- A pop-up message appears indicating that the *Security Desk* is trying to reconnect.
- The area view is unavailable.
- Previously displayed cameras remain connected.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 94 of 430

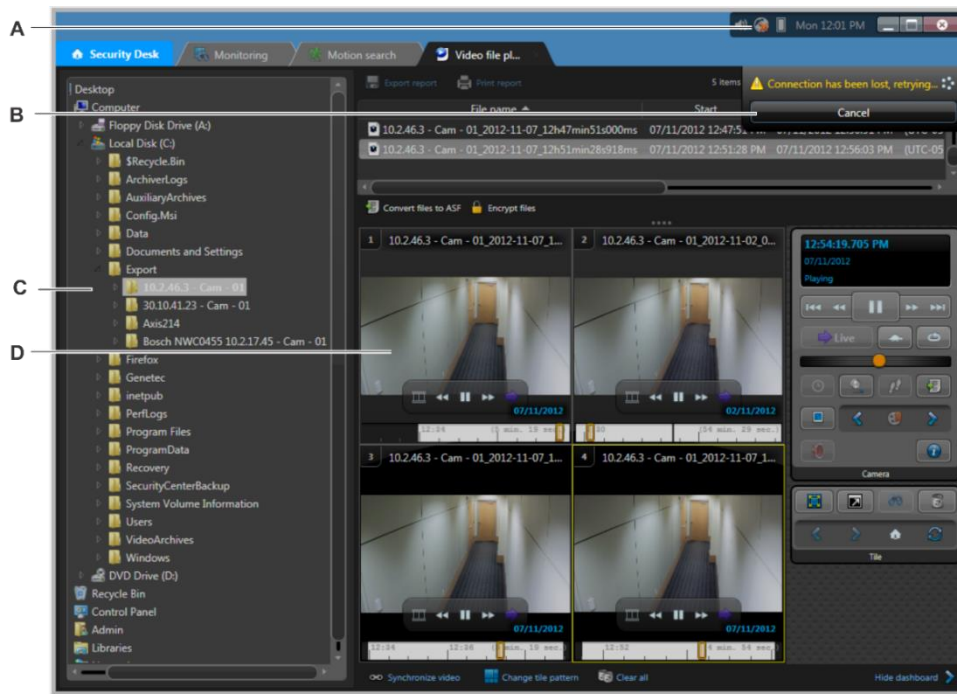


Figure 67. Directory Failure: Degraded Mode

In a multiple Directory server configurations, *Directory failover and load balancing* are managed by the **Directory Manager** role.

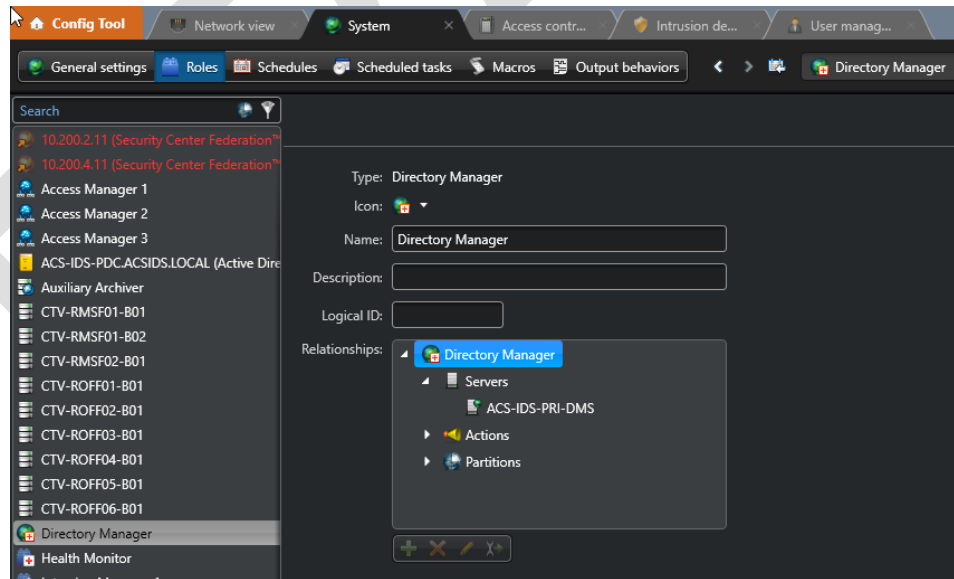


Figure 68. System Architecture: Directory Role

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 95 of 430

3.4.2 Archiver Role

The Archiver role is responsible for the discovery, status polling, and control of video units. The Archiver also manages the video archive and performs motion detection if it is not done on the unit itself.

All communications between the system and the video units are established through the Archiver role. All events generated by the units (motion, video analytics, and so on) are forwarded by the Archiver to the concerned parties on the system. Multiple instances of the Archiver role can be created on the system.

3.4.3 Access Manager Role

The **Access Manager** role manages and monitors access control units on the system. It keeps the units updated with the access control settings configured in *Security Center*, in real-time or on a schedule, so that they can make independent access control decisions whether they are connected to the Access Manager or not.

The Access Manager also logs the access control *events* in the database for access control investigation and maintenance reports. All events generated by the units (access granted, access denied, door open, etc.) are forwarded by the Access Manager, through the Directory, to the concerned parties on the system. Multiple instances of this role can be created on the system.

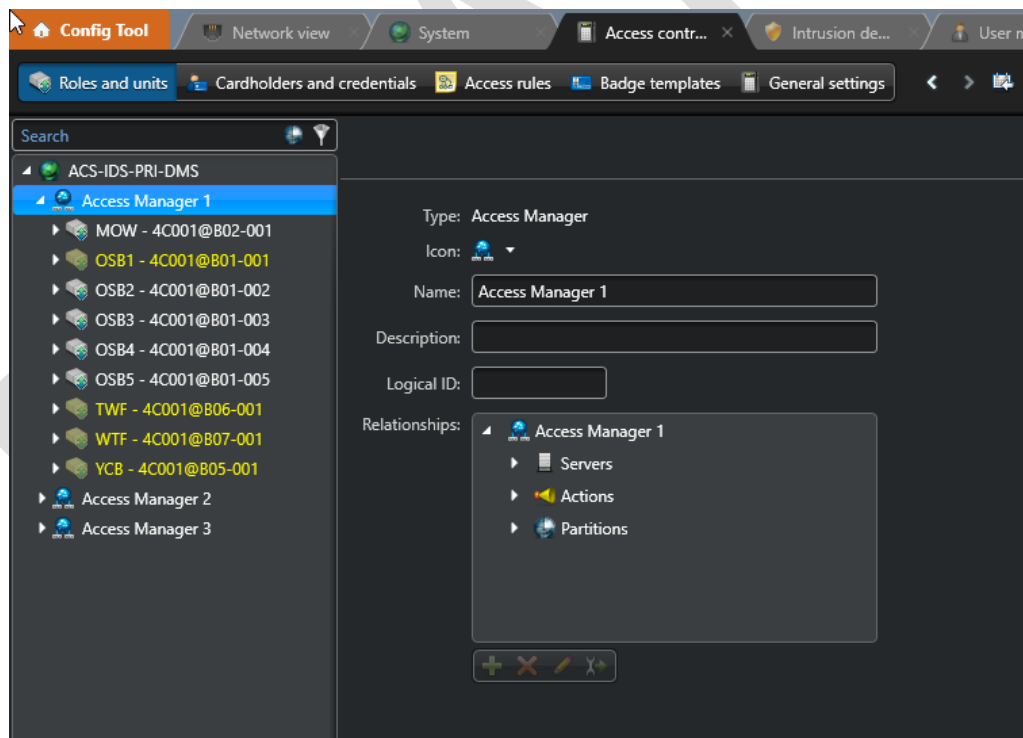


Figure 69. System Architecture: Access Manager Role

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 96 of 430

3.4.4 Media Router Role

The Media Router is the central role that handles all stream requests (audio and video) in the *Security Center*. It establishes streaming sessions between the stream source (camera or Archiver) and its requesters (client applications). Routing decisions are based on the location (IP address) and the transmission capabilities of all parties involved (source, destinations, networks, and servers).

The Media Router ensures all video streams use the best route to get to their destinations, while performing any necessary transformation (for example, from unicast to multicast, or from IPv4 to IPv6).

3.4.5 Zone Manager Role

Zone Manager is a type of role that manages virtual zones and triggers events, or output relays based on the inputs configured for each zone. It also logs the zone events in a database for zone activity reports. Multiple instances of this role can be created on the system.

3.4.6 Report Manager Role

Report Manager is a type of role that automates report emailing and printing based on schedules. Only one instance of this role is permitted per system. This role is created by default at system installation and hosted on your main server.

3.4.7 Health Monitor Role

The **Health Monitor** role monitors system entities such as servers, roles, units, and client applications for health issues. Health events are recorded in a database for the purpose of reporting and statistical analysis. Current system errors are reported in real-time in your application's notification tray. Only one instance of this role is permitted per system. It is created at system installation and cannot be deleted. From the **Health Monitor** role, you can choose which health events to monitor.

3.4.8 Map Manager Role

The Map Manager is the central role that manages all mapping resources in Security Center, including imported map files, external map providers, and KML objects. It acts as the map server to all client applications that require maps. You must configure this role before you can start using maps on your system.

3.4.9 Web-Based SDK Role

The Web-based SDK role exposes the Security Center SDK methods and objects as web services to support cross-platform development. It allows developers on platforms other than Windows (for example, Linux) to write custom programs that can interact with Security Center. This role mainly exists for clients who need custom development.

3.4.10 Plugin Roles

A plugin role adds optional features to the *Security Center*. A plugin role is created by using the **Plugin role template**. By default, it is represented by an orange puzzle piece (🧩) in the **Roles view** of the **System task**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 97 of 430

Plugin (with an uppercase, in singular) is the role template that serves to create specific plugin roles.

Create Plugin Roles (🔧)

Before you can create a plugin role, the software package specific to that role must be installed on your system. You must also make sure your *Security Center* license has a valid certificate for the plugin you want to use.

3.4.11 Role Failover

Failover is a backup operational mode in which a role (system function) is automatically transferred from its primary server to a secondary server that is on standby. This transfer between servers occurs only if the primary server becomes unavailable, either through failure or through scheduled downtime. Role failover is managed by the Directory role.

How Role Failover Works in Security Center

For failover to work in Security Center, you need to define the following two types of servers:

- **Primary server:** Server that normally hosts a role for it to work on the system.
- **Secondary server:** Servers on standby that are assigned to a role to keep it running in case the primary server becomes unavailable.

There is no limit to the number of secondary (or standby) servers you can assign to most roles. However, the more servers you add, the less cost-effective it might be for you.

The secondary server of one role can be the primary server of another role, provided that both servers have enough resources (CPU, memory, disk space, and network bandwidth) to handle the combined load of both roles in case of a failover.

- **IMPORTANT:** Security Center does not handle the failover of role databases. To protect your data, perform regular backups of the role database.

Before failover, a role is hosted on the *primary server* and connects to a *database server* hosted on a third computer. When the *primary server* fails, the role automatically fails over to the *secondary server* and reconnects to the **same** database server.

Before Failover		After Failover	
Primary server (hosting the role)	Secondary server (on standby)	Primary server (failed)	Secondary server (hosting the role)

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 98 of 430

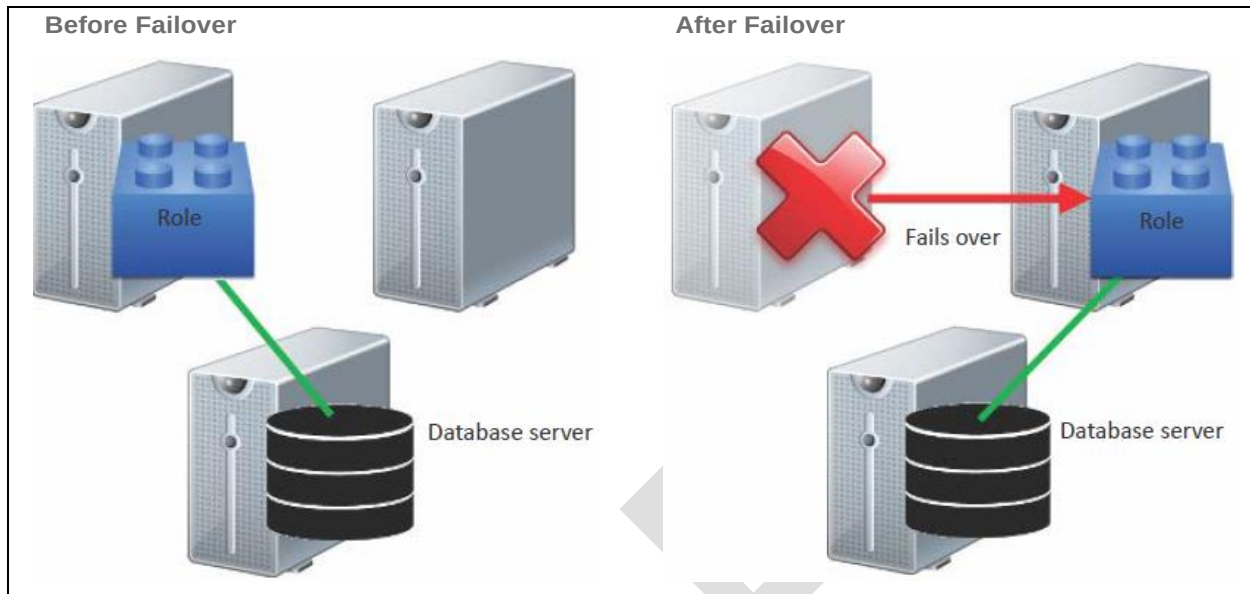


Figure 70. Role Failover

3.4.11.1 Roles Supporting Failover

Some roles in Security Center do not support failover, and others only support failover under certain conditions. [Table 31](#) lists which *Security Center* roles support failover, the failover approach they use, and any special requirements they might have.

Table 31. Security Center Roles that Support Failover

Role	Supports Failover	Comments and Exceptions
Access Manager		
Active Directory		
Active Directory Federation Services (ADFS)		The ADFS role runs on the same server as the Directory role. If Directory failover is configured, then the URL of every Directory server on your system must be added as endpoints to the <i>Security Center</i> relying party trust of the ADFS server that the ADFS role is connected to.
Archiver		Can have up to two secondary servers assigned to an Archiver role. Each server requires its own database, hosted locally, or on a separate computer.
Auxiliary Archiver	Not applicable	The function of the Auxiliary Archiver is to ensure that video archives remain available when the Archiver fails.
Directory	Yes	It can run simultaneously on up to five servers. It also supports the Directory database failover.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 99 of 430

Role	Supports Failover	Comments and Exceptions
Directory Manager	Not applicable	The function of the Directory Manager is to manage the Directory failover and load balancing.
Global Cardholder Synchronizer	Yes	
Health Monitor	Yes	
Intrusion Manager	Yes	Only when the intrusion panels are connected using IP. Failover is not supported if the intrusion panels are connected using serial ports.
Map Manager	Yes	BEST PRACTICE: It is best to set the map-cache to a location that can be reached by all servers assigned to the role.
Media Gateway	Yes	
Media Router	Yes	The primary and secondary servers can each have a separate database, hosted locally, or on another computer.
Omnicast™ Federation™	Yes	
Plugin	Yes	
Report Manager	Yes	
Security Center Federation™	Yes	
Web-based SDK	Yes	
Web Client Server	Yes	The Web Client must reconnect to a different URL when the role fails over to a different server.
Zone Manager	Yes	

3.4.11.2 Set Up Role Failover

To configure failover for roles on your system, you must select secondary servers to be on standby in case the primary server hosting the role becomes unavailable.

For roles that require a database (with the exception of the Archiver role), the database must be hosted on a different computer than any of the servers assigned to the role. All servers assigned to the role must be able to connect to the server managing the role database.

- **IMPORTANT:** All servers assigned to the same role must be running the same version of the *Security Center*.

To Set Up Role Failover:

1. From the **Config Tool** home page, open the **System** task, and click the **Roles** view.
2. Select the role you want to configure failover for, and then click the **Resources** tab where the role's primary server is listed
3. Under the **Servers list**, click **Add an item** (+).

A dialog box opens, listing all remaining servers on your system that are not yet assigned to this role.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 100 of 430

- Select the server that you want to add as a secondary server and click **Add**.

The secondary server is added below the primary server. The green LED indicates which server is hosting the role.

NOTE: The servers are listed in the order that they are picked if a failover occurs. When the primary server fails, the role automatically switches to the next server on the list.

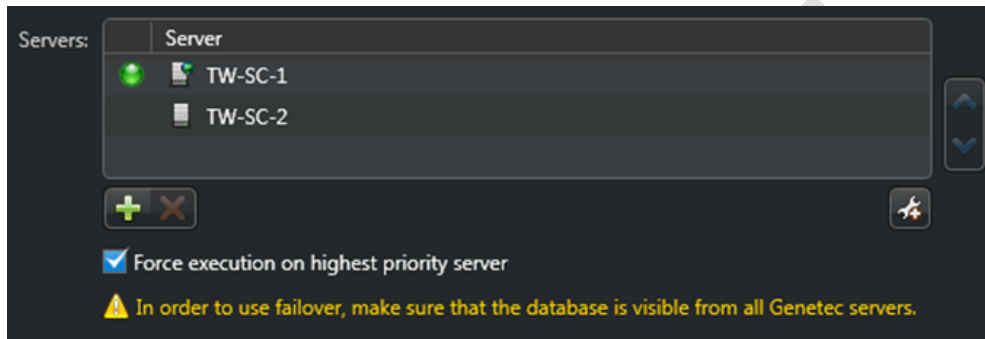


Figure 71. Failover: Secondary Server

- To change the priority of a server, select it from the list, and click the (⬆️) or (⬇️) buttons to move it up or down the list.
- If you want the primary server to retake control after it is restored from a failover, select the **Force execution on highest priority server** option.

To minimize system disruption, the role remains on the secondary server after a failover occurs, by default.

- Click **Apply**.

3.4.11.3 Change the Server Priority for Role Failover

You can make secondary servers into primary servers or ensure that a primary server is always the one hosting the role as long as it is running.

To minimize system disruption, the role remains on the secondary server after a failover occurs, by default. You can change the server priority and force the highest priority server to always be the one hosting the role.

To Change the Server Priority for Failover

- From the **Config Tool** home page, open the **System task**, and click the **Roles** view.
- Select the role and then click the **Resources** tab where the role's primary server is listed.
- Select a server from the list and click the (⬆️) or (⬇️) buttons to change the server priority. The higher a server is in the list, the higher its priority.
- Select the **Force execution on highest priority server** option and click **Apply**.

This option forces the server with the highest priority (at the top of the list) to always be the one hosting the role, as long as it is online. If the first server is offline, then the priority goes to the second server on the list, and so on and so forth.

After a few seconds, the green LED moves to the server that is at the top of the list, indicating that it is now the one hosting the role.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 101 of 430

- **IMPORTANT:** Servers are displayed in the order they are picked if a failover occurs. When the primary server fails, the role automatically switches to the next server in the list.

3.4.12 Deactivate and Activate Roles

For maintenance or troubleshooting purposes, you can deactivate a role without affecting any of its settings and then re-activate it later.

If you are experiencing issues with your system, sometimes it is helpful to restart a role. Roles are also deactivated so their properties can be modified. For more information about configuring roles in **Config Tool**, see the *Security Center Administrator Guide*.

You must be a system administrator to deactivate or activate a role.

To Deactivate a Role:

1. From the home page, open the **System status** task.
2. From the **Monitor** drop-down list, select **Roles**.
3. The roles that are part of your system are listed in the report pane.
4. Select a role you want to deactivate and click **Deactivate role** (🛑).
5. The role turns red (inactive) in the report pane.
6. To reactivate the role, select the role, and click **Activate role** (🟢).

3.4.13 Move Roles to Other Servers

You can move a role to another server without installing any additional software, for example, if the server that the role is installed on is slow or has limited disk space. Make sure you have another server configured and ready to accept a new role. Moving a role to another server might cause a short pause in the role's operations.

- **NOTE:** This procedure does not apply to Archiver roles.

To Move a Role to Another Server:

1. From the **Config Tool** home page, open the **System** task, and click the **Roles** view.
2. Select the role you want to modify, and then click the **Resources** tab.
3. If the role requires a database, do one of the following:
 - If the database resides on a third computer, you have nothing to change.
 - If the database is empty, you can create it anywhere you want.
 - If the database contains data and is residing on the current server, move the database to the new server or to a third computer.
4. Under the **Servers** list, click **Add an item** (+).
- A dialog box appears with all available servers on your system.
5. Select the substitute server and click **Add**.
6. Select the current server in the Servers list and click **Delete** (✖).
7. Click **Apply**.

3.4.14 Connect Roles to Remote Database Servers

If a role's database is hosted on a different computer than the role, you must configure the remote

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 102 of 430

database server (SQL Server) to accept connection requests from the role.

On the computer hosting SQL Server, open TCP ports 1433 and 1434 on Windows Firewall.

To Connect a Role to a Remote Database Server:

1. Allow remote connection on your SQL Server instance.
 - A. On the server hosting the database, open *Microsoft SQL Server Management Studio* and connect to the database server used by *Security Center*.
 - B. In the **Microsoft SQL Server Management Studio** window, right-click the database server name in the **Object Explorer** and select **Properties**.
 - C. In the **Server Properties** window, select the **Connections** page.
 - D. Under the section **Remote server connections**, select the option **Allow remote connections to this server**.
 - E. Click **OK** and close *Microsoft SQL Server Management Studio*.
2. Enable **Named Pipes** and **TCP/IP** protocols on your SQL Server instance.
 - A. On the server hosting the database, open *SQL Server Configuration Manager*.
 - B. Expand the **SQL Server Network Configuration** section and select the protocols for your database server instance (for example, **Protocols for SQLEXPRESS**).
 - C. Right-click the **Named Pipes** and **TCP/IP** protocols, and set their status to **Enabled**.

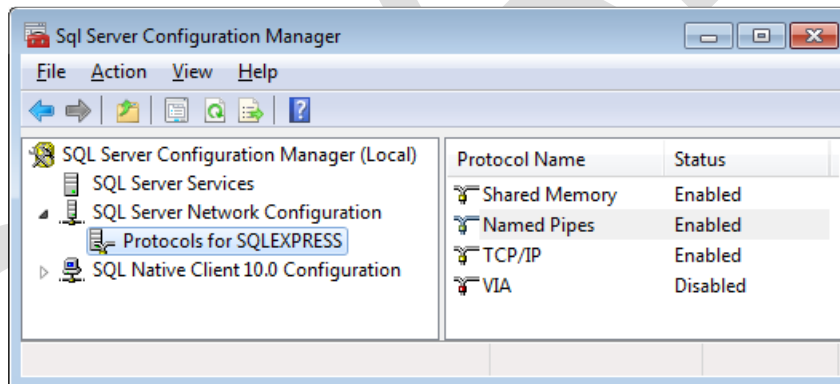


Figure 72. SQL Server Configuration Manager

- D. Close *SQL Server Configuration Manager*.
3. Make sure your SQL Server instance is visible from other computers on your network.
 - A. On the server hosting the database, open *Microsoft Management Console Services* (services.msc).
 - B. Start the service named **SQL Server Browser**.
 - C. Right click the SQL Server Browser service and click **Properties**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 103 of 430

- D. In the **General** tab, from the **Startup type** drop-down list, select **Automatic**. The SQL Server instance is now available from the Database server drop-down list of any role's **Resources** tab in **Config Tool**.
4. Restart your SQL Server instance to enable the settings you have changed.
 - A. On the server hosting the database, open Microsoft Management Console Services (services.msc).
 - B. Right-click the SQL Server instance service (for example, SQL Server (SQLEXPRESS)) and click **Restart**.
 5. On every server that hosts your *Security Center* roles, change the login user of the **Genetec Server** service to a Windows administrator account that also has the permissions to access the SQL Server instance you just modified.
The Windows administrator account is usually a domain account used to connect to all servers.
 - A. On the server hosting the role, open *Microsoft Management Console Services* (services.msc).
 - B. Right-click the **Genetec Server** service and click **Properties**.
 - C. In the **Log on** tab, select the This account option, and type an administrator **Account name** and **Password**.
 - D. Click **Apply > OK**.
 - E. Repeat these steps on every server that is hosting a *Security Center* role that will connect to the remote database server.
 6. Select the role in **Config Tool > Resources** tab and modify the database path to point to the remote database.

3.5 ACCESS CONTROL

This section describes

- Access Control Units
- Access Control Entries
- Access Controllers
- Access Managers
- Access Manager and Access Logic
- Access Control Task

3.5.1 Access Control Units

An access control unit is a type of entity that represents an intelligent access control device, such as a Synergis™ appliance or an HID network controller, that communicates directly with the **Access Manager** over an IP network. An access control unit operates autonomously when it is disconnected from the Access Manager.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 104 of 430

3.5.1.1 Investigate Events Related to Access Control Units

You can investigate events related to access control units, using the **Access control unit events** report. For example, you can use the **Access control unit events** report to see if any critical events happened relating to access control unit in the last week (for example, Hardware tamper), by searching for that event and setting the time range.

To Investigate Access Control Unit Events:

- From the home page, open the **Access control unit events** task.
- Set up the query filters for your report. Choose one or more of the following filters:
 - Access control units:** Select the access control units to investigate.
 - Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
 - Events:** Select the events of interest. The event types available depend on the task you are using.
 - Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the previous week or the previous month.
- Click **Generate report**. The access control unit events are listed in the **Report** pane.
 - NOTE:** If you have **Access Managers** that are offline when you launch the query, you'll get an error message for each one of them, even though they are not related to the selected access control units. This is because the system has no way of knowing whether the selected units were managed by one of them in the past or not.

3.5.1.2 Report Pane Columns for the Access Control Unit Events Task

After generating a report, the results of your query are listed in the **Report** pane. This section lists the columns available for the relevant reporting task.

- Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- Event:** Event name.
- Event timestamp:** Date and time that the event occurred.
- Occurrence period:** Period when the event occurred.
- Product type:** Model of the unit involved.
- Tamper:** Name of the interface module that has been tampered with.
- Unit:** Access control, video, or intrusion detection unit involved.

3.5.1.3 View Input/Output (I/O) Configuration of Access Control Units

You can view the I/O configurations (controlled access points and doors) of access control units, using the **I/O configuration** report. For example, you can use the **I/O configuration** report to search for a specific door and see how the access through each door side is configured (REX, readers, I/O modules, and so on).

To View the I/O Configuration of An Access Control Unit:

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 105 of 430

1. Open the **I/O configuration** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
 - **Access control units:** Select the access control units to investigate.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
 - **Devices:** Select the devices to investigate.
 - **Location:** Specify the areas where the devices are located.
3. Click **Generate report**. The input and output configurations of the selected access control units are listed in the **Report** pane.

3.5.1.4 Report Pane Columns for the I/O Configuration Task

After generating a report, the results of your query are listed in the **Report** pane. This section lists the columns available for the relevant reporting task.

- **Access point:** Access point involved (only applicable to areas and doors).
- **Access Manager:** Access Manager controlling the unit.
- **Controlling:** Door controlled by the device.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **IP address:** IP address of the unit or computer that generated the event.
- **Manufacturer:** Manufacturer of the unit.
- **Physical name:** Device name.
- **Unit:** Access control, video, or intrusion detection unit involved.
- **Unit type:** Type or model of unit involved.

3.5.1.5 Enable External Access Control Devices

You can enable and disable external access control devices, such as USB readers, signature pads, card scanners, and so on, from the **Options** dialog box. These settings are saved locally for your Windows user profile. For information about the access control devices available, see your manufacturer documentation.

To Enable or Disable External Access Control Devices:

1. From the home page, click **Options > External devices**.
2. Next to each external device, set the option **ON** or **OFF**.
3. Click **Save**.
4. Restart your application.

3.5.2 Access Control Entities

[Table 32](#) provides a list of entities you can create.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 106 of 430

Table 32. Access Control Entities

Icon	Entity	Description
	Access Manager (role)	Role that manages the door controllers in the system.
	Access control unit	Door controller that a reader is attached to.
	Door	Physical barriers controlled by an access control unit.
	Access rule	The logic used to determine whether or not to grant access.
	Secured area	Physical location whose access is controlled by access rules and other access control behavior, such as antipassback, interlock, first-person rule, two-person rule, and so on.
	Cardholder	Individual who possesses a credential.
	Cardholder group	Group of cardholders sharing common characteristics
	Credential	The claim of identity, such as a card, PIN, biometric scan, and so on.
	Badge template	Custom-designed printing template for user credentials.
	Schedule	Date and time range.
	Partition	Group of entities on the system visible only to a group of users.
	User	Individual who uses <i>Security Center</i> applications.
	User group	Group of users sharing common characteristics

3.5.2.1 How Access Events Display in Tiles

A tile is an individual window within the canvas, used to display a single entity. The entity displayed is typically the video from a camera, a map, or anything of a graphical nature. The look and feel of the tile depend on the displayed entity.

Tiles can display the following:

- Entities
- Event information
- Live and playback video
- Video images
- Cardholder pictures and information
- LPR reads
- Web pages
- Tile plugins
- Maps

Content is automatically displayed in tiles when events occur related to the entities you are monitoring. You can also display entities by dragging them into a tile. *Security Desk* tiles have a tile-memory, meaning that Security Desk remembers the last 8 entities displayed in each tile. Using the commands in the **tile** widget, you can switch to the **previous**, **next**, and **initial tile content**.

You can right-click inside the tile to view tile menu commands.

[Figure 73](#) shows a tile displaying a camera.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 107 of 430

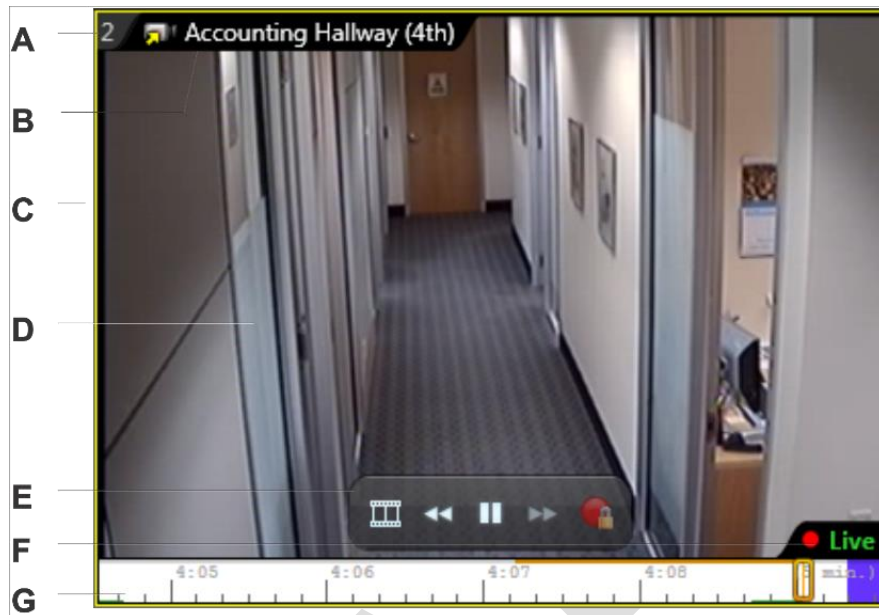


Figure 73. Tile Displaying A Camera

The letters below correspond to [Figure 73](#).

- A. **Tile ID:** The tile ID is the number displayed at the upper left corner of the tile. This number uniquely identifies each tile within the canvas. If the tile ID is blue, it means event monitoring is enabled for the tile. If it is black, monitoring is disabled. If it is red with a narrow band of blue, event and alarm monitoring are enabled for the tile.
- B. **Tile toolbar:** Displays the entity name. When an event occurs, information corresponding to the event is also shown in the tile toolbar.
- C. **Yellow frame:** Indicates that the tile is selected.
- D. **Video stream:** The streaming video is displayed inside the tile. Double-click to expand the tile to the whole canvas.
- E. **On-tile video controls:** Use the on-tile video controls while viewing the video in a tile.
- F. **Recording state:** Recording state is the current recording status of a given camera. There are four possible recording states: Enabled, Disabled, Currently recording (unlocked), and Currently recording (locked). Green indicates that it is not recording. Red indicates that it is recording.
- G. **Timeline:** A timeline is a graphic illustration of a video sequence, showing where in time, motion, and bookmarks are found. Thumbnails can also be added to the timeline to help the user select the segment of interest. Use the timeline to control playback video.

You can customize what to show in the canvas tiles from the **Options** dialog box.

The parts of a tile that can be hidden are the timeline, on-tile video controls, tile toolbar, and tile ID. The tile settings are saved as part of your user profile.

The parts of a tile that can be hidden are the **timeline**, **on-tile video controls**, **tile toolbar**, and tile ID. The tile settings are saved as part of your user profile.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 108 of 430

To Customize How Tiles Display:

1. From the home page, click **Options > Visual**.
2. From the **Display timeline** drop-down list, select when to show the timeline in tiles, in live, and in playback:
 - **Auto-hide:** Only show the timeline when the mouse cursor hovers inside the tile boundaries.
 - **Always:** Always show the timeline.
 - **Never:** Never show the timeline.
3. To show the on-tile video controls when you hover your mouse cursor inside a tile (play, pause, and so on), select the **Display overlay video controls** option.
4. To show an entity's full path with the entity name in the tile toolbar, select the **Display entity names** with their full path option.

An entity's path is the hierarchy of areas above that entity in the area view. When the path is too long, an "*" is displayed instead.

Example: "Montreal office/Main entrance", or "*/*/Back entrance".

NOTE: This option also applies to alarms. When this option is selected, the full path of the entity that triggered the alarm is displayed in the Source column in the **Monitoring** task and **Alarm monitoring** task.

5. To show the **Tile** toolbar only when you hover your mouse cursor over a tile, select the **Auto-hide tile toolbar** option. When this option is cleared, the tile toolbar is always displayed.
6. To show the **tile ID** number only when you hover your mouse cursor over the tile, select the **Auto-hide tile number** option.
7. When this option is cleared, the **tile ID** is always displayed.
8. Click **Save**.

3.5.2.2 Tile Menu Commands

You can control your tiles and the entities displayed in tiles using commands in the tile menu. Some commands always appear, and other contextual commands change depending on the entity type displayed in the tile. lists the commands available from the tile menu.

Table 33. Tile Menu Commands

Command	Description
 Start Incident Recording	Start recording the video related to every entity that is placed in the tile (cameras, areas, doors, cardholders, and so on), to Create an incident report package.
 Maximize Tile	Expand the current tile to fill the canvas. Hides all other tiles.
 Maximize Tile Fullscreen	Hide the area view and dashboard, and make the current tile fill the canvas. Forces the tile to be displayed in full-screen mode.
Navigate	
 Back	Show previous tile content.
 Forward	Show the next tile content.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 109 of 430

Command	Description
 Home	Show initial tile content.
 Refresh	Refresh tile content.
 Clear All	Empty all content from tiles.

3.5.2.3 Viewing Entities in the Canvas

You can view an entity in a canvas tile from the area view or the **report** pane. All entities listed in the area view and some entities and events in the **report** pane can be viewed in a canvas tile, with the exception of the **System entity** (). Entities can also appear automatically in a tile when an event occurs. If it is helpful for you, you can show more information next to the entities in the area view by customizing how entities are displayed.

To View an Entity in the Canvas:

- From the area view or the **report** pane, do one of the following:
 - To view a single entity, double-click or drag the entity into a tile.
 - To view multiple entities, hold **CTRL** or **SHIFT**, select the entities, and drag them into a tile. This method only works if there enough free tiles.
- To control the entities, right-click inside the tile and use the tile menu commands or use the widgets in the dashboard.
- To clear entities from the canvas, do one of the following:
 - Right-click on a tile, and then click **Clear** ().
 - Select a tile, and then press the **BACKSPACE** key.
 - (Empties all tiles) At the bottom of the canvas, click **Clear all** ().
 - (Empties all tiles) Press **CTRL+BACKSPACE**.

3.5.2.4 Unpack Content in Tiles

When an entity is displayed in a tile that has other entities associated with it, you can unpack the entity and view all the attached entities in separate tiles.

Entities that have two or more entities attached to them are called composite entities (for example, a door that has multiple cameras associated to it). If you are monitoring the door and an event occurs at the door, only the first camera is displayed because the multiple cameras are packed. If you unpack the door, you can view all the cameras in separate tiles.

To Unpack Content in a Tile:

- Select a tile that is displaying a composite entity.
- Beside the entity name in the tile toolbar, click ().
- From the drop-down menu, click one of the following:

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 110 of 430



Figure 74. Unpack Content in a Tile

- An attached camera (in the example, Main Entrance or Front Hallway).
 - **Unpack**: View all entities attached to the selected entity in separate tiles.
 - **Start cycling**: Rotate through the entities that are attached to the composite entity within the tile.
4. To repack the tiles when you have finished viewing what you need to see, click **Pack** (🔒) in the upper-left corner of the tile. The amount of time each entity is displayed can be configured from the **Options** dialog box.
- **NOTE**: If there is a **PTZ** camera attached to the composite entity and you start controlling the PTZ, the cycling stops. You can click **Start cycling** again once you are done controlling the PTZ.
 - **Example**: The Main Entrance door has two cameras associated to it: the Main Entrance camera and the Front Hallway camera. An Access denied event occurs at the main door, and the event is displayed in a tile. Since the tile is packed, only the first camera is displayed (Main Entrance), until you unpack the tile content.

Customize Entity Cycling Options

You can select how many seconds *Security Desk* dwells on each entity when rotating through composite entities (such as an alarm, area, or a camera sequence) in a tile. This setting is saved as part of your user profile.

To Customize Entity Cycling Options:

1. From the home page, click **Options > General**.
2. In the **Dwell time** section, set the **Entity cycling** value.
3. Click **Save**.

3.5.3 Access Controllers

The access control unit, or, a door controller is physically wired to various door components:

- The reader

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 111 of 430

- The lock
- The door monitor
- The request to exit
- A buzzer/horn

The access control unit is connected to the Access Manager over IP.

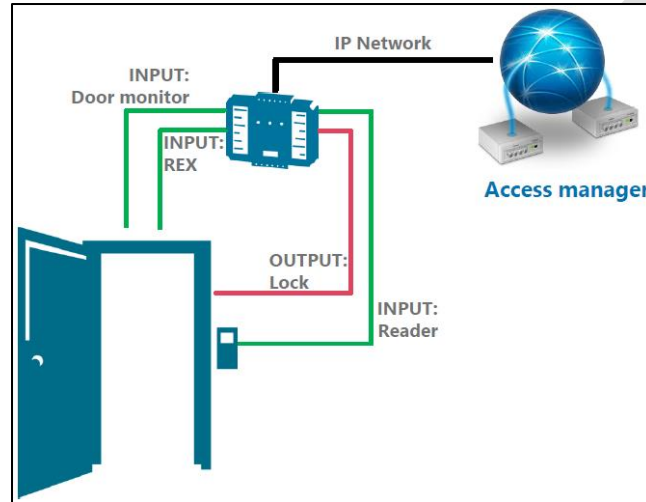


Figure 75. Access Controller

3.5.4 Access Managers

The Access Manager role manages and monitors access control units on the system. The Access Manager keeps the units updated with the access control settings configured in Security Center, in real-time or on a schedule, so that they can make independent access control decisions whether they are connected to the Access Manager or not.

The Access Manager also logs the access control events in the database for access control investigation and maintenance reports. All events generated by the units (access granted, access denied, door open, etc.) are forwarded by the Access Manager, through the Directory, to the concerned parties on the system. Multiple instances of this role can be created on the system.

3.5.4.1 Access Manager and Doors

[Figure 76](#) shows an example of how the Access Manager:

- Establishes a TCP connection to each controller for command & control.
- Pushes access control logic down to the door.
- Receives door events from controller.
- Maintains a database of historical door events

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 112 of 430

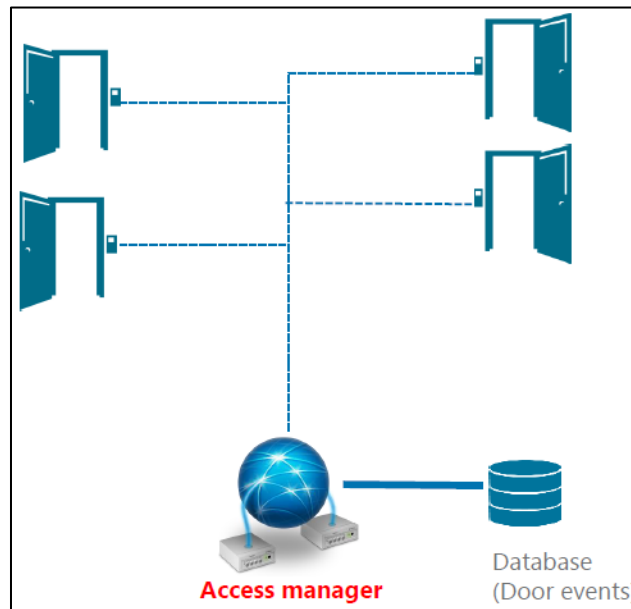


Figure 76. Access Manager and its Doors

3.5.4.2 Configure Access Manager Roles

To monitor the units, keep them in sync with the access control settings in Security Center, and allow them to make access control decisions independently, you can configure an Access Manager to control the units.

When *Synergis™* is enabled in your license, an Access Manager role is created by default and hosted on the main server.

To Configure an Access Manager Role:

1. From the **Config Tool** home page, open the **Access control** task, and click the **Roles and units** view.
2. Select the **Access Manager** role to configure and click **Resources**.
3. If necessary, configure the database required to run this **Access Manager**.
4. Click **Properties** and configure the general settings of the **Access Manager**.
 - **Keep events:** Specify how long you want to keep the events in the Access Manager database before deleting them. The access control event are used for reporting and maintenance purposes (they include events related to doors, areas, and other access control entities).
 - **Indefinitely:** Keep the events until you manually delete them.
 - **For:** Select the number of days for the retention period.
 - **CAUTION:** If you are using the SQL Server 2014 Express database engine (included with the Security Center installation files), the database size is limited to 10 GB. A door event uses (on average) 200 bytes in the database. If you configure the Access Manager to

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 113 of 430

keep door events indefinitely, the database eventually reaches the 10 GB limit and the engine stops.

- **Activate peer to peer:** Select this option to enable the communication between Synergis™ units managed by this Access Manager.
 - **BEST PRACTICE:** Only enable peer to peer communication if you plan to create I/O zones that involve multiple Synergis™ units or apply antipassback to areas controlled by multiple Synergis™ units. Leave this option off for better system security and performance.
- **Activate global antipassback:** Select this option if you need to apply antipassback to areas controlled by multiple Synergis™ units. To enable this option, you must first enable peer to peer.
 - **BEST PRACTICE:** If all your antipassback areas are controlled by a single unit, do not enable global antipassback. Enabling global antipassback increases the communication between Synergis™ units.
- 5. If necessary, add the extensions for the access control unit types that you want this **Access Manager** to manage.
- 6. Add the access control units that you want this **Access Manager** to manage.

After you finish, if you need more than one **Access Manager** role on your system, you can create additional **Access Manager** roles and host them on separate servers.

3.5.5 Access Manager and Access Logic

- A. Access configurations are done on the workstation
- B. The workstation is connected to the Directory
- C. The Directory saves the configuration in its database
- D. The Directory sends the configuration to the Access manager
- E. The Access manager pushes the settings over TCP to the controller(s)
- F. The controllers save the settings locally at the door

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 114 of 430

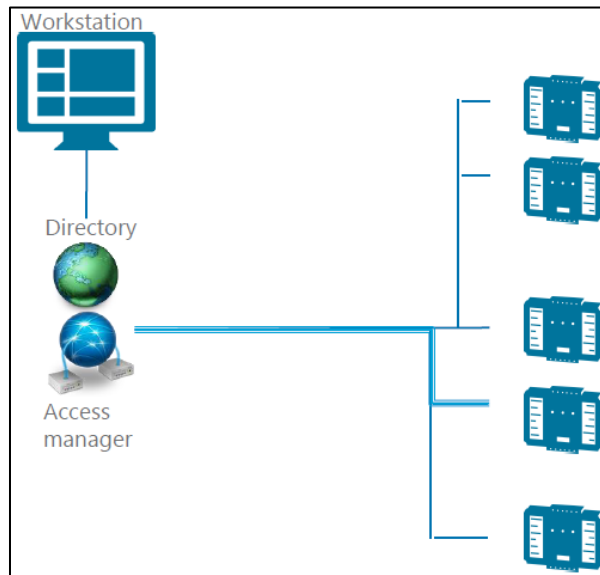


Figure 77. Access Manager and Access Logic

3.5.6 Access Control Task

The cardholder management task displays a flat list showing:

- Cardholder
- Picture
- Cardholder group
- Last access
- Etc. (customizable)

Cardholders can be created, deleted, modified here:

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 115 of 430

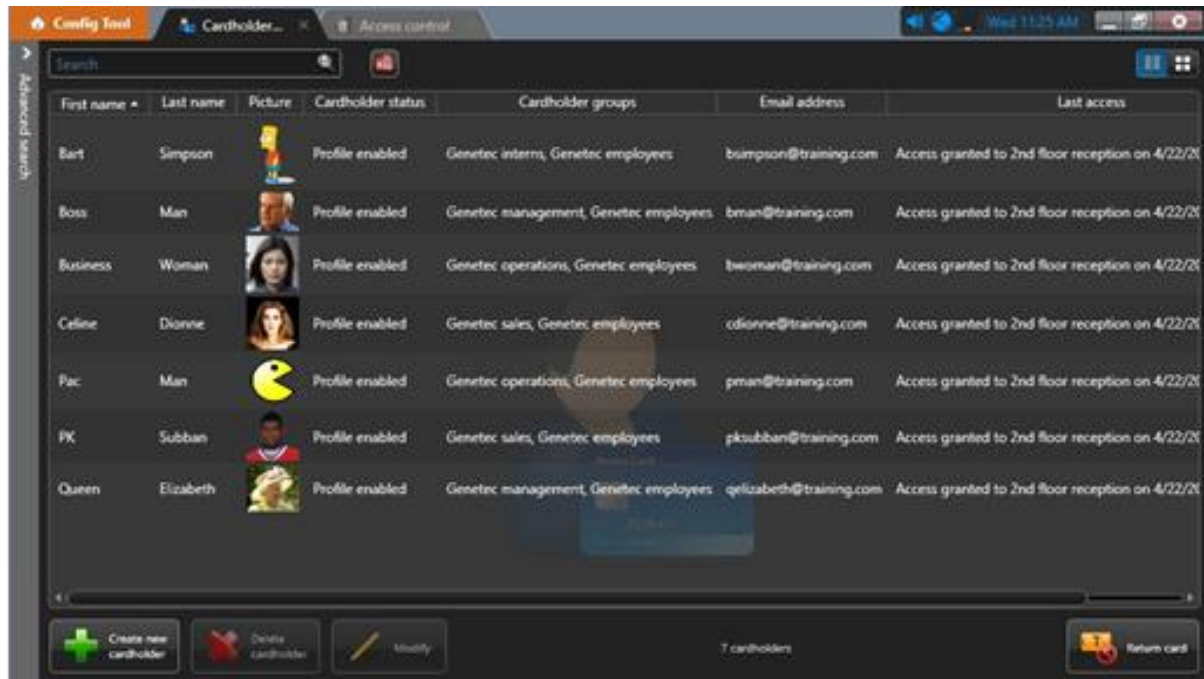


Figure 78. Access Control Rules: Access Control Task

3.6 ACCESS RULES

An access rule is a type of entity that defines a list of cardholders to whom access is either granted or denied based on a schedule. An access rule can be applied to a secured area or to an access point. An access rule contains the three W's:

- Who? (Who can pass through - cardholders or cardholder groups)
- What? (Whether access is granted or denied)
- When? (The schedule when the access rule is applied)

This logic is different from other access control solutions, where an access level defines where and when someone can gain access.

Access rules that have been pushed to the door controllers (called access control units in Security Center) do not have to be modified. If you associate a new credential with a cardholder, the old rule is still valid. They provide the basic logic by which access will be controlled.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 116 of 430

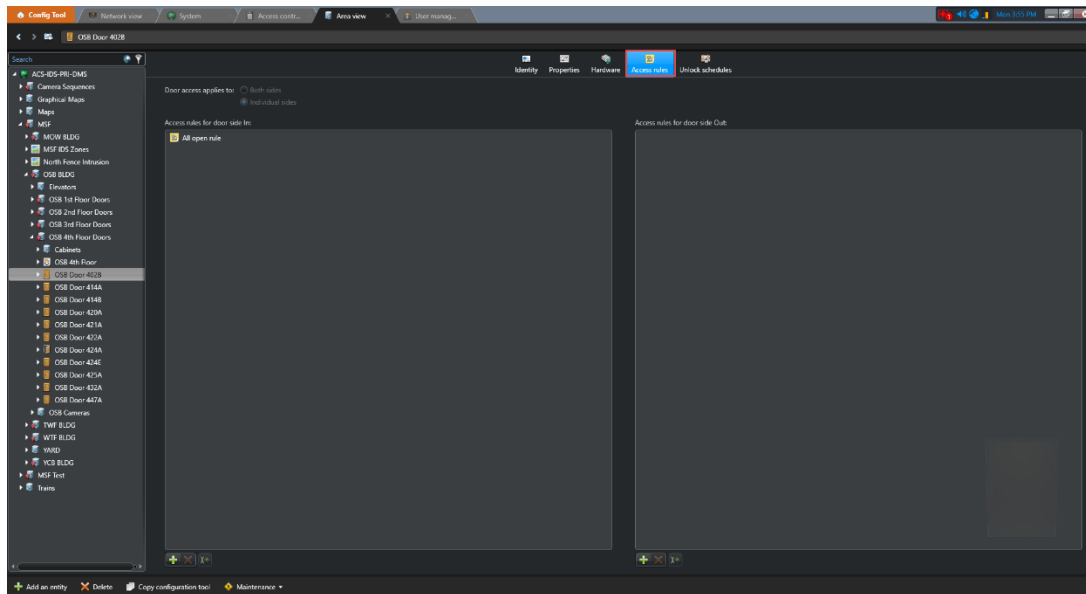


Figure 79. Access Control Configuration: Area View: Access Rules

Access rules are created in the **Config Tool's Access control** task.

- **Access rule configuration:** Access rule configuration is a type of maintenance task that reports on entities and access points affected by a given access rule.
- **Access troubleshooter:** Access troubleshooter is a tool that helps you detect and diagnose access configuration problems. With this tool, you can find out about the following:
 - Who is allowed to pass through an access point at a given date and time?
 - Which access points a cardholder is allowed to use at a given date and time.
 - Why a given cardholder can or cannot use an access point at a given date and time.
- **Action:** An action is a user-programmable function that can be triggered as an automatic response to an event, such as door held open for too long or object left unattended, or that can be executed according to a specific time table.
- **Active alarm:** An active alarm is an alarm that has not yet been acknowledged.

From the **Config Tool** home page, open the **Access control** task, and click the **Access rules view**. Click **Access rule** (). Assign a name and description to the access rule.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 117 of 430

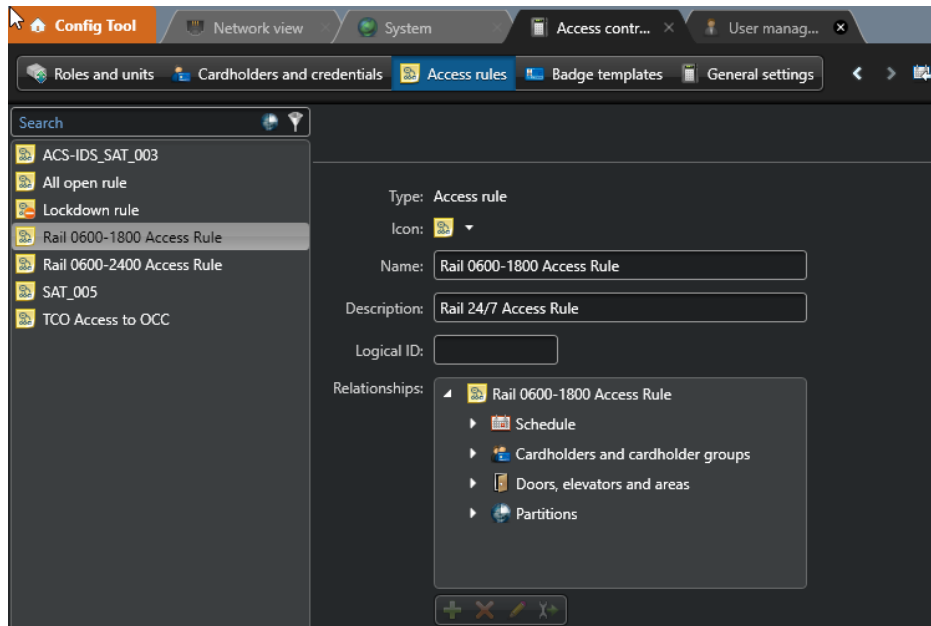


Figure 80. System Architecture: Access Rules

Permanent vs. Temporary Access Rules

Access rules are either permanent or temporary. A temporary access rule is an access rule that has an activation and an expiration time. Temporary access rules are suited for situations where permanent cardholders need to have temporary or seasonal access to restricted areas. These access rules are automatically deleted seven days after they expire to avoid cluttering the system.

Typical use case examples of temporary access rules include seasonal cardholders, such as students who need to access a lab during their semester, and permanent cardholders who need short term access to a restricted area, such as maintenance technicians who need to work on storage servers at a highly secured data center.

From the Cardholder management task, you can only assign a temporary access rule to one cardholder at a time. To assign a temporary access rule to multiple cardholders or cardholder groups, you must update the access rule properties from Config Tool.

Limitations

Temporary access rules work with both HID and Synergis™ units. However, only Synergis™ units can apply temporary access rules while operating offline (disconnected from the Access Manager). For HID units to work with temporary access rules, the controller must always be connected to the Access Manager, and the synchronization must be set to Automatically. The activation of temporary access rules is immediate because of the host lookup. However, the expiration of a temporary access rule only comes in effect after a synchronization with the Access Manager.

3.6.1 Assign Access Rules to Cardholders

To grant or deny a cardholder access to areas and doors, you must assign access rules to them.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 118 of 430

Create access rules

You can assign access rules while you are creating cardholders, or after they are created. In this procedure, it is assumed you have already created a cardholder.

- **BEST PRACTICE:** Assign access rules to cardholder groups, rather than to individual cardholders. Assign access rules to individual cardholders only as a temporary measure. When used too often, the access control system can quickly become unmanageable. If you need to grant temporary or short-term access to a cardholder, create a temporary access rule.

To Assign Access Rules to a Cardholder:

1. In the **Cardholder management** task, select a cardholder, and then click **Modify** (✎).
2. Click the **Access rules** (🔑) tab > **Add** (+). A dialog box listing the access rules that are not yet assigned to this cardholder opens.
3. Do one of the following:
 - Select the rule you want to add and click **Add**.
 - Create and assign a temporary access rule.
4. Select the access rule from the list.

The schedule that applies to the access rule is shown in a grid on the right. Each time block represents 30 minutes. Green areas indicate periods when access is granted by the rule. Red areas indicate periods when access is denied by the rule. Grey areas are times not specified by the schedule; therefore, access is denied. If it is a temporary access rule (🕒), the activation and expiration times are indicated. Areas and doors that the rule is associated with are listed at the bottom.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 119 of 430

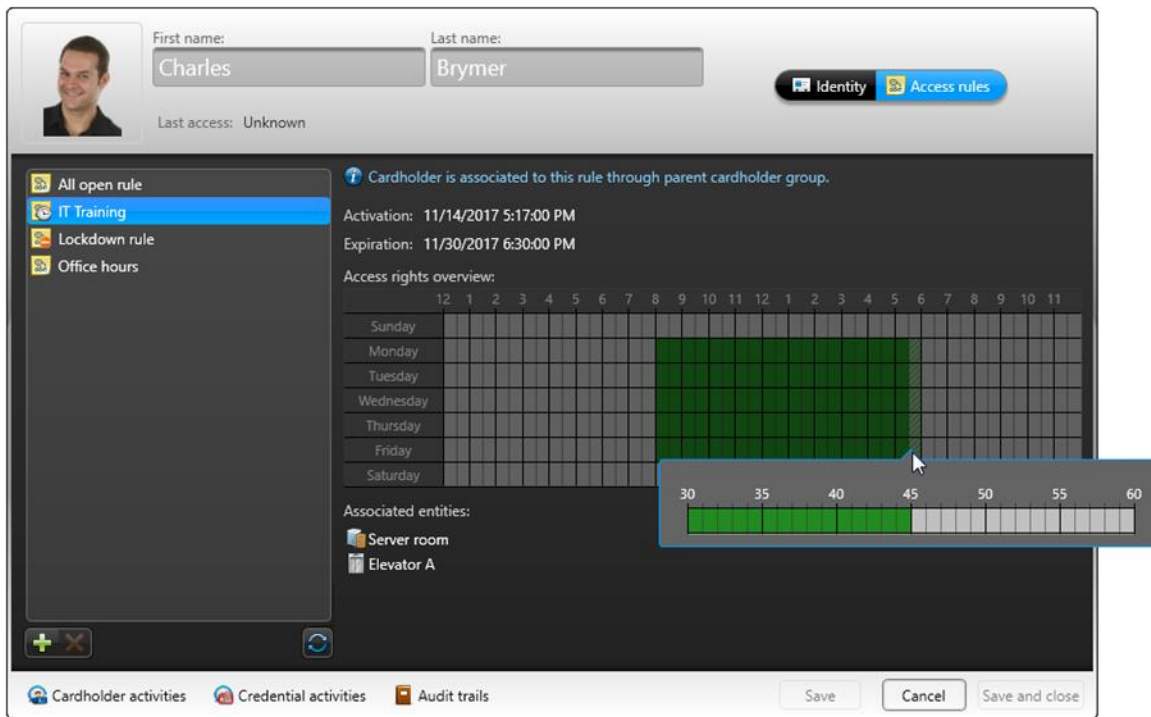


Figure 81. Access Rules: Scheduling

5. To view a partial (hatched) time block in minutes, click and hold the left mouse button.
6. To assign another access rule to the cardholder, click (+).
7. To remove an access rule directly assigned to the cardholder, click (X). You cannot remove the *All open rule*, or the *Lockdown rule*.
8. Click **Save**.
9. After you finish assign a credential to the cardholder.

3.6.2 Assign Temporary Access Rules to Cardholders

To accommodate seasonal cardholders, such as students who are enrolled during a semester, or permanent cardholders who need short term access to a restricted area, you can create and assign temporary access rules.

A temporary access rule is an access rule that has an activation and an expiration time. Temporary access rules are suited for situations where permanent cardholders need to have temporary or seasonal access to restricted areas. These access rules are automatically deleted seven days after they expire to avoid cluttering the system.

- **NOTE:** From the Cardholder management task, you can only assign a temporary access rule to one cardholder at a time. To assign a temporary access rule to multiple cardholders or cardholder groups, you must update the access rule properties from Config Tool. For Security Desk users to able to create temporary access rules, you need to grant them the Add access rules privilege.

To Assign a Temporary Access Rule to a Cardholder:

1. In the **Cardholder management** task, select a cardholder, and then click **Modify** (✎).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 120 of 430

2. Click the **Access rules** (🔑) tab > **Add** (+). A dialog box listing the access rules that are not yet assigned to this cardholder opens.
3. Do one of the following:
 - Select an existing temporary access rule (🔑) and click **Add**.
 - Click **Temporary access rule** (+). The **temporary access rule creation** wizard opens.
4. In the **Basic information** page, enter the rule name and description, then click **Next**.
5. In the **Access rule information** page, do one of the following:
 - Click **Use an existing access rule as template**, then select from the **Access rule** drop-down list, the access rule you want to use as template.
 - The schedule and the associated entities will be copied to your temporary access rule.
 - Click **Specify custom access parameters**, and specify the following:
 - **Access to:** Expand the area view and select the entities you want to grant access to.
 - **Activation:** Activation date and time, or when the rule schedule starts to apply.
 - **Expiration:** Expiration date and time, or when the rule schedule stops to apply.
 - **Schedule:** Choose when this access rule is active.
6. Click **Next** > **Create**. A temporary access rule (🔑) is created and assigned to your cardholder.
7. Click **Save**.
8. After you finish assign the temporary access rule you created to other cardholders.

3.6.3 Identify who Is Granted Access to Doors

You can verify which cardholders are granted access to a particular door side at a specific date and time, using the **Door troubleshooter** report. This report is helpful, because it allows you to see what the configuration of a door is and determine if their properties must be adjusted. The door troubleshooter does not examine each cardholder's credentials. You can further diagnose the cardholder's access rights using the **Access troubleshooter** tool.

To Identify Who is Granted Access to a Door:

1. From the home page, open the **Door troubleshooter** task.
2. In the **Filters** tab, select a date and time for the report.
3. Select a door you want to investigate.
4. From the **Access point drop-down** list, select the access point (door side) you want to verify.
5. Click **Generate** report.

All cardholders who can go through the selected access point at the specified time are listed in the report pane.

After you finish, if necessary, test your access control configuration.

3.6.4 Identify Who is Granted/Denied Access at Access Points

You can find out which cardholders are currently granted or denied access to selected areas or doors, using the **Cardholder access rights** report.

This report is helpful because it allows you to see where a cardholder can go, and when, and

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 121 of 430

determine if their access rule properties must be adjusted.

TIP: Perform your query on one access point at a time, so your report is more specific.

To identify who is granted/denied access at an access point:

1. From the home page, open the **Cardholder access rights** task.
2. Set up query filters for your report. Choose one or more of the following filters:
 - **Doors - Areas:** Restrict the search to activities that took place at certain doors and areas.
3. Click **Generate report**.
 - The cardholders associated with the selected access point through an access rule are listed in the report pane. The results indicate if the cardholder is granted or denied access, and by which access rule.
4. To show a cardholder in a tile, double-click or drag a cardholder from the report pane to the canvas.
5. To view additional cardholder information in the tile, click (i).

After you finish, if necessary, modify the cardholder's access rights.

3.6.5 Identify Which Entities Are Affected by Access Rules

You can find out which entities and access points are affected by a given access rule, using the Access rule configuration report. In the report results, you can see the members of the access rule, such as the cardholders, doors, and the associated schedule. This helps you determine if you must add or remove entities or adjust the schedule.

To Identify Which Entities are Affected by an Access Rule:

1. Open the **Access rule configuration** task.
2. Set up the query filters for your report. Choose one or more of the following:
 - **Access rule:** Select the access rule to investigate.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity and if the custom field was made visible to you when it was created or last configured.
3. In the **Expand cardholder groups** option, select **Enable** to list the members of the affected cardholder groups in the report instead of the cardholder groups themselves.
4. In the **Include perimeter entities** option, select **Enable** to include the perimeter entities of the affected areas in the report.
5. Click **Generate report**.

The entities and access points affected by this access rule are listed in the **report** pane.

Report Pane Columns for the Access Rule Configuration Task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Access point:** Access point involved (only applicable to areas and doors).
- **Access rules:** Name of the access rules.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 122 of 430

- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity and if the custom fields were made visible to you when they were created or last configured.
- **Icon:** Graphical representation of the affected entity type.
- **Member:** Name of the affected entity.
- **Type:** Affected entity type.

3.6.6 Enable External Access Control Devices

You can enable and disable external access control devices, such as USB readers, signature pads, card scanners, and so on, from the **Options** dialog box.

These settings are saved locally for your Windows user profile. For information about the access control devices available, see your manufacturer documentation.

To Enable or Disable External Access Control Devices:

1. From the home page, click **Options > External devices**.
2. Next to each external device, set the option **ON** or **OFF**.
3. Click **Save**.
4. Restart your application.

3.6.7 Investigate Events Related to Access Control Units

You can investigate events related to access control units, using the **Access control unit events** report. For example, you can use the **Access control unit events** report to see if any critical events happened relating to access control unit in the last week (for example, Hardware tamper), by searching for that event and setting the time range.

To Investigate Access Control Unit Events:

1. From the home page, open the **Access control unit events** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
 - **Access control units:** Select the access control units to investigate.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity and if the custom field was made visible to you when it was created or last configured.
 - **Events:** Select the events of interest. The event types available depend on the task you are using.
 - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time, such as the previous week or the previous month.
3. Click **Generate report**. The access control unit events are listed in the report pane.
 - **NOTE:** If you have **Access Managers** that are offline when you launch the query, you'll get an error message for each one of them, even though they are not related to the selected access control units. This is because the system has no way of knowing whether the selected units were managed by one of them in the past or not.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 123 of 430

3.6.7.1 Report Pane Columns for the Access Control Unit Events Task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity and if the custom fields were made visible to you when they were created or last configured.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **Occurrence period:** Period when the event occurred.
- **Product type:** Model of the unit involved.
- **Tamper:** Name of the interface module that has been tampered with.
- **Unit:** Access control, video, or intrusion detection unit involved.

3.6.8 View I/O Configuration of Access Control Units

You can view the I/O configurations (controlled access points, and doors) of access control units, using the I/O configuration report. For example, you can use the I/O configuration report to search for a specific door and see how the access through each door side is configured (REX, readers, I/O modules, and so on).

To View the I/O Configuration of an Access Control Unit:

1. Open the **I/O configuration** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
 - **Access control units:** Select the access control units to investigate.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity and if the custom field was made visible to you when it was created or last configured.
 - **Devices:** Select the devices to investigate.
 - **Location:** Specify the areas where the devices are located.
3. Click **Generate report**.

The input and output configurations of the selected access control units are listed in the report pane.

3.6.8.1 Report Pane Columns for the I/O Configuration Task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Access point:** Access point involved (only applicable to areas and doors).
- **Access Manager:** Access Manager controlling the unit.
- **Controlling:** Door controlled by the device.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity and if the custom fields were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **IP address:** IP address of the unit or computer that generated the event.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 124 of 430

- **Manufacturer:** Manufacturer of the unit.
- **Physical name:** Device name.
- **Unit:** Access control, video, intrusion detection unit involved.
- **Unit type:** Type or model of the unit involved.

3.6.9 Test Cardholder Access Rights

You can find out which access points a cardholder is allowed to use at a given date and time, using the **Cardholder troubleshooter** tab in the **Access troubleshooter** tool.

The cardholder troubleshooter does not examine each cardholder's credentials. You can further diagnose the cardholder's access rights by clicking the **Access diagnosis** tab.

To Troubleshoot a Cardholder's Access Rights:

1. From the home page, click **Tools > Access troubleshooter**
2. In the **Access troubleshooter** dialog box, click the **Cardholder troubleshooter** tab.
3. Select the date and time you want the troubleshooter to base its evaluation on. Only access rules are evaluated based on the specified date and time.
4. Select the cardholder that you want the troubleshooter to examine. Instead of a cardholder, you can also select a credential or a visitor.
5. The entities that are currently inactive are greyed out.
6. Click **Go**.

The access points that the selected cardholder (or visitor) has the right to use at the specified time, based on the current access rules, are listed.

3.6.9.1 Test Cardholder Access Rights Based on Credentials

You can diagnose why a cardholder with a given credential can, or cannot access a given door, at a given date and time, using the **Access diagnosis** tab in the **Access troubleshooter** tool.

To Test a Cardholder's Access Rights Based on their Credential:

1. From the home page, click **Tools > Access troubleshooter**.
2. In the **Access troubleshooter** dialog box, click the **Access diagnosis**  tab.
3. Select the date and time you want the troubleshooter to base its evaluation on.
4. Select the cardholder you want to examine. Instead of a cardholder, you can also select a credential or a visitor.
5. If the selected cardholder has more than one credential, specify the one you want to examine.
6. Select an access point to examine. If you select a door, specify a door side.
7. Click **Go**.

The troubleshooter produces a diagnosis based on the current system configuration, taking into consideration the access rules, and both the cardholder's and the credential's activation and expiration dates.

3.6.10 Test Access Rules at Doors

You can find out who has the right to pass through a door side at a given date and time, using the **Access troubleshooter** tool. The door troubleshooter does not examine each cardholder's

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 125 of 430

credentials. You can further diagnose the cardholder's access rights by clicking the **Access diagnosis** tab (🔍).

To Test the Access Rules at a Door:

1. From the home page, click **Tools > Access** troubleshooter.
2. In the **Access troubleshooter** dialog box, click the **Door troubleshooter** tab.
3. Select the date and time you want the troubleshooter to base its evaluation on. Only access rules are evaluated based on the specified date and time.
4. Select the access point that you want the troubleshooter to examine:
 - If you select a door, specify a door side.
5. Click **Go**.

The active cardholders who have the rights to use the selected access point at the specified time, based on the current access rules, are listed.

3.6.11 Optional Access Rules

An access rule is a type of entity that defines a list of cardholders to whom access is either granted or denied based on a schedule. An access rule can be applied to a secured area or to an access point.

3.6.11.1 Deny Rule

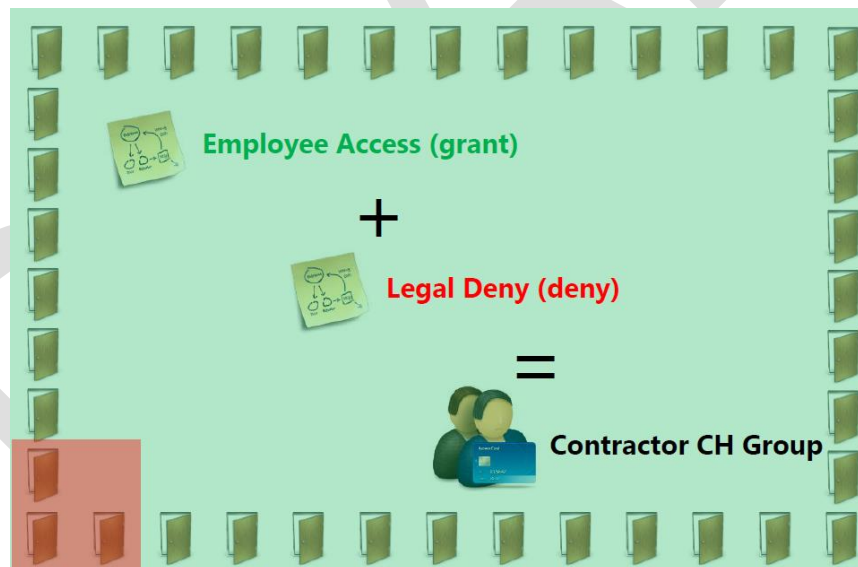


Figure 82. Access Rules: Deny Rule

3.6.11.2 Temporary Access Rule

A temporary access rule is an access rule that has an activation and an expiration time. Temporary access rules are suited for situations where permanent cardholders need to have temporary or seasonal access to restricted areas. These access rules are automatically deleted seven days after

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 126 of 430

they expire to avoid cluttering the system.

3.6.11.3 Cardholders and Rules

Access rules define who can gain access through which door(s).

Access rules name cardholders (or groups), not cards.

3.7 CARDHOLDER MANAGEMENT

Cardholder management is a type of operation task that allows you to create, modify, and delete cardholders. In this task, you can also manage a cardholder's credentials, including temporary replacement cards.

The cardholder management task displays a flat list showing:

- First Name
- Last Name
- Cardholder Picture
- Cardholder Status
- Cardholder Group
- Email Address
- Last Access

Cardholders can be created, deleted, modified here.

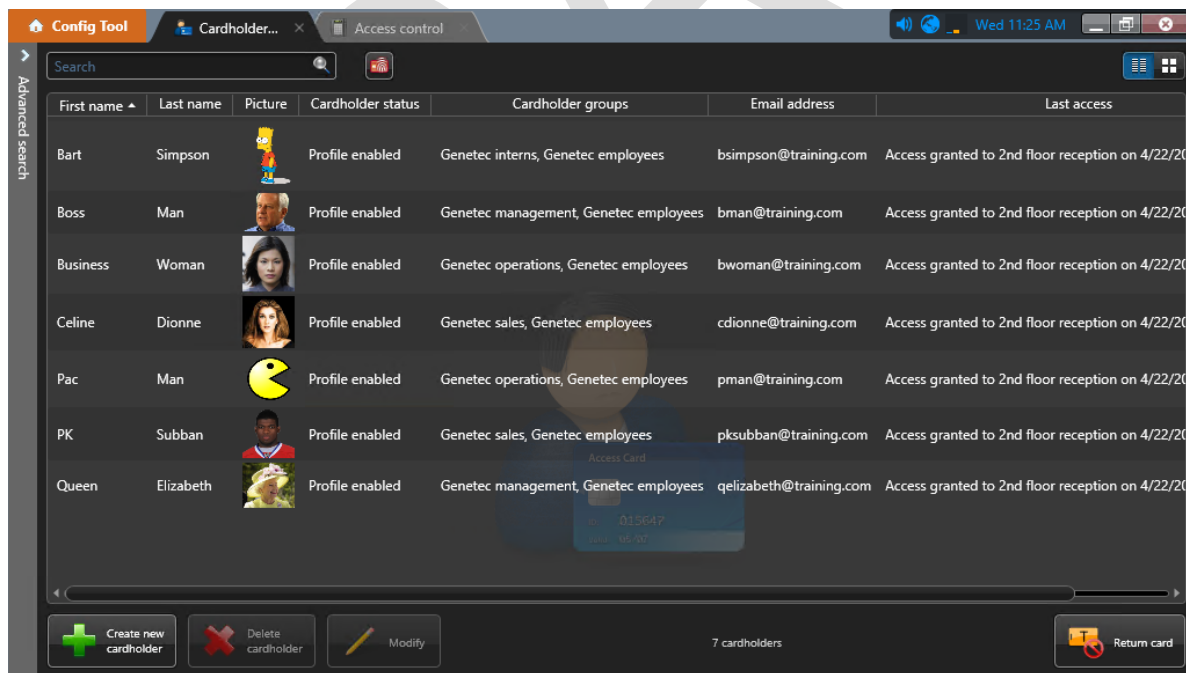


Figure 83. Cardholder Management Task

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 127 of 430

3.7.1 Cardholders

A cardholder is a type of entity that represents a person who can enter and exit secured areas by virtue of their credentials (typically access cards) and whose activities can be tracked.

3.7.1.1 Create a Cardholder

To add new employees who must enter and exit secured areas using access cards, and to track their activities, you can create cardholders using the **Cardholder management** task.

- To add custom information to cardholders, create custom fields in **Config Tool** (see the *Security Center Administrator Guide*).
- If you require different groups of cardholders with different access rights, create cardholder groups in **Config Tool** (see the *Security Center Administrator Guide*).

To Create a Cardholder:

- Open the **Cardholder management** task and click **Create new cardholder** (+).
- At the top of the dialog box, enter the cardholder's first name and last name.
- To assign a picture to the cardholder, click the silhouette and select one of the following options:
 - Load from file:** Select a picture from disk. All standard image formats are supported.
 - Load from webcam:** Take a snapshot with your webcam. This option appears only if you have a webcam attached to your workstation.
 - Load from camera:** Take a snapshot from a camera managed by *Security Center*. When you click **Load from camera**, a separate capture dialog box opens. Select the video source and click **Take snapshot** (📷).
 - Load from clipboard:** Load the picture copied to the clipboard. This option appears only if you used the **Windows copy** command to save a picture onto your clipboard.
- To edit the picture, click it to open the **Image editor** and use the editing options at the top of the **editor's** dialog box.
- In the **Status** section, set the following:
 - Status:** Set their status to Active or Inactive. For their credentials to work, and for them to have access to any area, their status must be Active.
 - Activation:** If their status is currently set to Inactive, set a date and time to activate their profile.
 - Expiration:** Set an expiration for their profile:
 - Never:** Never expires.
 - Specific date:** Expires on a specific date and time.
 - Set expiration on first use:** Expires after a specified number of days after the first use.
 - When not used:** Expires when it has not been used for a specified number of days.
- Assign a credential to the cardholder so they can access secured areas.
 - NOTE:** You can assign a credential now or after all credentials have been enrolled in the system.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 128 of 430

7. Assign the cardholder to a cardholder group.

NOTE: A cardholder can belong to more than one cardholder group.

- To assign the first cardholder group, click the Cardholder group drop-down list and select a cardholder group.
- To assign additional cardholder groups, click **Advanced** (+), then click **Add an item** (+). In the dialog box that opens, select the cardholder groups, and click **OK**.

8. Enter the cardholder's email address.

A valid email address is necessary if you want to assign mobile credentials to the cardholder.

9. Optional: If custom fields are defined for cardholders, such as department, phone numbers, and so on, enter the additional cardholder information.

10. Optional: In the **Advanced** section, configure the following cardholder properties:

NOTE: Some of these properties can be inherited from the parent cardholder groups. When a specific value is configured for the cardholder, click **Revert to inherited value** (+) to inherit the property from the parent cardholder groups. If multiple parent groups exist, the most privileged value is inherited.

A. If the cardholder has been assigned a credential, grant access privileges to the cardholder:

- Use extended grant time: Grants them more time to pass through doors where the **Extended grant time** parameter is configured for a door. Use this option for those with reduced mobility.
- Bypass antipassback rules: **Exempts them from all antipassback restrictions.**
- To learn more about configuring areas and doors using the extended grant time and antipassback rules, see the *Security Center* Administrator Guide.**

B. In the **Security clearance** field, enter the cardholder's security clearance level. The security clearance level determines their access to areas when a threat level is set in *Security Center*. Level 0 is the highest clearance level, with the most privileges.C. In the **Entity name** field, type a name for the **cardholder** entity, if you do not want to use the cardholder's name. By default, the **Entity name** uses the **First name** and **Last name** fields.

- In the **Description** field, type a description for the cardholder.
- Assign the cardholder to a partition.

Partitions determine which *Security Center* users have access to this entity. Only accepted users of the partition can view or modify the cardholder.

11. Click **Save**.

3.7.1.2 Assign Access Rules to Cardholders

You can assign access rules while you are creating new cardholders, or after they are created. In this procedure, it is assumed you have already created a cardholder.

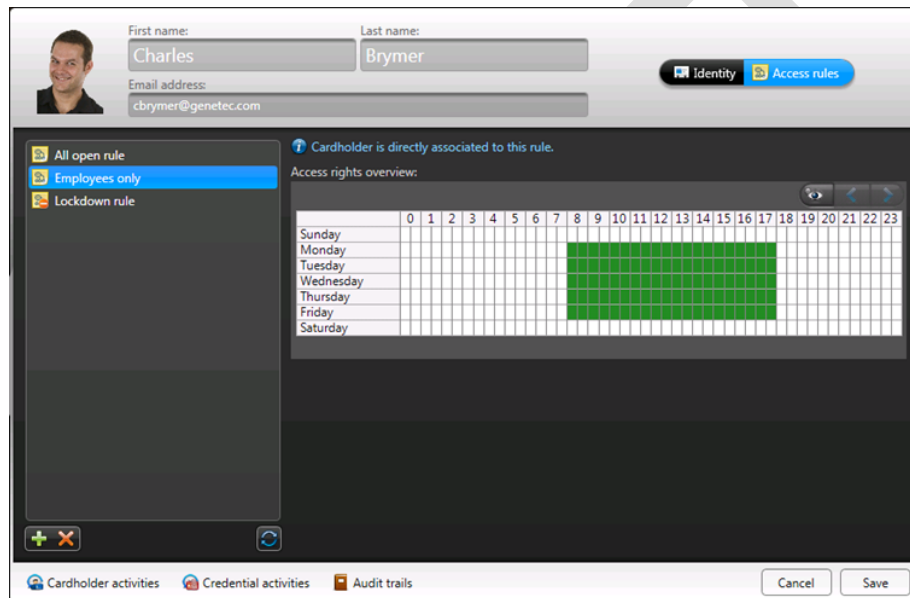
- BEST PRACTICE:** Assign access rules to cardholder groups, rather than to individual cardholders. Assign access rules to individual cardholders only as a temporary measure. When used too often, the access control system can quickly become unmanageable.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 129 of 430

To Assign Access Rules to a Cardholder:

1. In the **Cardholder management** task, select a cardholder, and then click **Modify** (✎).
2. Click the **Access rules** (🔑) tab > **Add** (+). A dialog box that lists all access rules in the system opens.
3. Select the rule you want to add and click **Add**.
4. Select the **access rule** from the list.

The schedule that applies to the access rule is shown in a grid on the right. Green areas indicate periods when access is granted by the rule. Red areas indicate periods when access is denied by the rule. White areas are times not specified by the schedule; therefore, access is denied.

**Figure 84. Access Rights Overview**

5. To view the access rule schedule in minutes, click (👁). Use the arrow buttons to scroll left or right.
6. To assign another access rule to the cardholder, click (+).
7. To remove an access rule directly assigned to the cardholder, click (✖). You cannot remove the **All open** rule, or the **Lockdown** rule.
8. Click **Save**.

3.7.1.3 Crop Pictures

To cut out an area of a cardholder's picture and focus on the part of the image that you would like to keep, you can crop the picture using the **Image editor**.

To Crop a Picture:

1. Click the picture.
2. In the Image editor, click the **Crop** (📏) tab.
3. On the image, click and drag the (📏) icon to crop the picture.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 130 of 430

4. To adjust the crop area, do one of the following:
 - Use the blue icons on the image to adjust the crop area.
 - At the bottom of the **Image editor** dialog box, use the **Width** and **Height** values to resize the crop area. The width and height values can be in pixels, inches, or millimeters.



Figure 85. Image Editor

5. To revert the picture to its original state, click **Reset**.
6. Click **Apply**.

3.7.1.4 Apply Transparent Backgrounds to Pictures

If a cardholder's picture was taken in front of a chroma key screen, you can make the picture background transparent. This is helpful if you create a badge template that has an image in the background.

To apply a transparent background to a picture:

1. Click the picture.
2. In the Image editor, click the **Transparency** tab.
3. The cursor changes to the **eyedropper** tool when you point to the image.
4. Click the background where the chroma color is (usually green or blue).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 131 of 430



Figure 86. Picture Background: Chroma Color

5. Using the **Tolerance slider**, adjust the transparency percentage.



Figure 87. Picture Background: Transparent

6. To revert the picture to its original state, click **Reset**.
7. Click **Save**.

3.7.1.5 Define the Maximum File Size of Pictures

To improve the sharpness of the cardholder pictures, you can increase the maximum file size for pictures that are stored in the **Directory** database.

The maximum file size applies to cardholder pictures and to all image data fields in *Security Center*. This setting also applies to the Import tool and can be modified while running this tool. When loading image files, *Security Center* automatically reduces the image size so that their file size is under the limit you set.

The default value is 20 KB. You can set the limit anywhere between 20 and 5000 KB.

To Define the Maximum File Size of Pictures:

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 132 of 430

1. Open the **Access control** task and click the **General settings** view.
2. In the **Maximum picture file size** option, set the maximum number of kilobytes.
3. Click **Apply**.

The new limit will apply to all future image field updates.

3.7.1.6 Assign Credentials

To grant cardholders access to secured areas, you must assign them credentials. Cardholders can be assigned multiple credentials. You can assign credentials while you are creating a new cardholder (except for mobile credentials), or after they have been created. In this procedure, it is assumed you have already created the cardholders.

To Assign Credentials:

1. Do one of the following:
 - For cardholders, open the **Cardholder management** task, select a cardholder, and then click **Modify** (✎).
2. In the **Credential** section, click **Add a credential** (+).
3. Select one of the following options:
 - **Automatic entry**: Present the card at a reader.
 - **Manual entry**: Manually enter the card data. Use this method when you do not have a card reader near you.
 - **Existing credential**: Select a pre-enrolled, unassigned credential.
 - **PIN**: Create a PIN credential.
 - **Request card**: Request a credential card for the cardholder. Use this method if you do not have a printer on site.
 - **Mobile credential**: Request a mobile credential for the cardholder. You must have a mobile credential provider set up, and mobile credential readers installed. The cardholder must have a valid email address configured.
 - **Paper credential (print)**: Print a badge (name tag or photo ID card) without assigning a credential. The paper credential cannot be used to open doors. It is only used to visually identify the cardholder.
4. If you select **Automatic entry**, you must then select a reader (USB reader or a door) and present the card at the reader.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 133 of 430

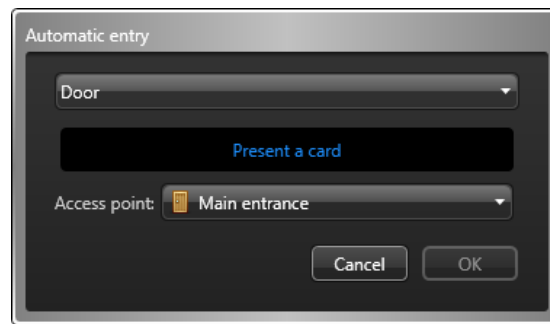


Figure 88. Automatic Entry

If you have a smart card encoding reader set up, set the option **Encode** before enrollment to **OFF** to read a pre-encoded card.

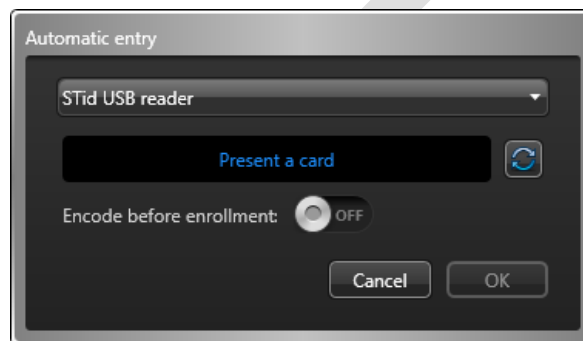


Figure 89. Encode OFF

When the reader LED turns green (ready to read), place the smart card on the reader. The reader LED turns yellow and then green with a short beep before turning off.

If you want to generate and encode on your card a random 128-bit DESFire EV1 credential before enrolling it, set the option **Encode before enrollment** to **ON**.

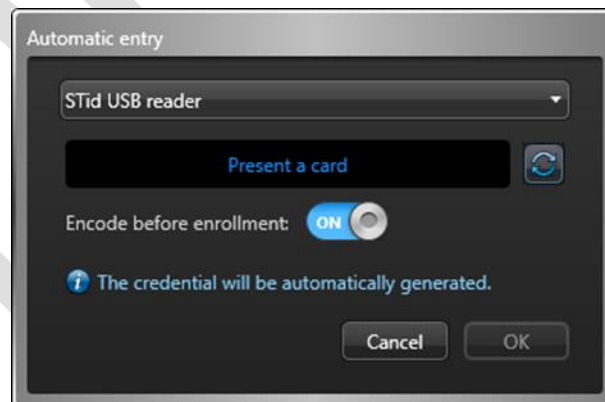


Figure 90. Encode ON

When the reader LED turns red (ready to encode), place the smart card on the reader for approximately 2 seconds. The reader LED turns yellow and then green with a short beep

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 134 of 430

before turning off. If you hear a long beep and the LED stays red, try again.

The dialog box closes automatically after an eligible card is presented. If the card has not been enrolled, it is enrolled automatically. If the card was already assigned to someone, it is rejected.

5. If you select **Manual entry**, you must then select a card format, enter the required data fields, and click **OK**.

Figure 91. Manual Entry

- **CAUTION:** Enter your card data carefully, because the system cannot validate whether the data you entered correspond to a physical card or not.
 - If the card has not been enrolled, it is enrolled automatically. If the card was already assigned to someone, it is rejected.
6. If you select **Existing credential**, a dialog box listing all existing but unassigned credentials in the system appears. Select an unassigned credential from the list and click **OK**.
 7. If you select **PIN**, you must then do the following:
 - A. Enter the **PIN** as a numerical value.

NOTE: Do not exceed the number of digits accepted by your readers. A typical PIN length is five digits. But certain models accept up to 15 digits.

- B. Click **OK**.

Figure 92. Cardholder Enter a PIN

8. If you select **Mobile credential**, you must then do the following:

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 135 of 430

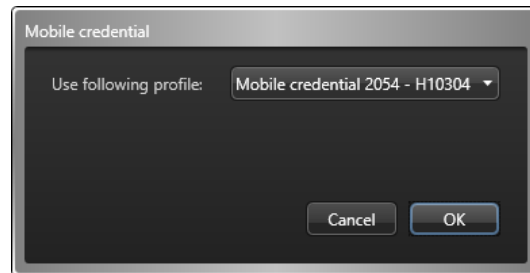


Figure 93. Mobile Credential

- A. Select the credential profile (if there is more than one).

You can assign one mobile credential from each profile to the cardholder.

- B. Click **OK**.

- **NOTE:** An email invitation is sent to the cardholder with a link to download the mobile credential app. The cardholder must accept the invitation for the credential to be activated on their phone. If the cardholder declines the invitation or if the invitation times out, the credential remains unused, and the mobile credential provider can assign it to the next cardholder who needs one. *Security Center* does not know that the requested mobile credential has not been accepted by the cardholder until the same mobile credential is assigned to someone else, at which time, *Security Center* automatically removes it from the current cardholder.
- **IMPORTANT:** A mobile credential that has been activated (paired to a phone) can never be reused on another phone. If a cardholder loses their phone or needs to change their phone, they must inform the *Security Center* operator who must delete the credential or flag it as lost. After that, the operator must log on to the credential provider's portal and revoke the mobile credential.

9. After the credential is assigned, it appears in the **Credential** section.

The credential name and status are displayed. **Active** indicates the credential is assigned.

- **NOTE:** If the credential is a PIN, the keypad icon is displayed. If the credential is a card, a default badge template is assigned, and a print preview of the badge is displayed instead of the credential icon.

10. Optional: If the credential is a card, select a different badge template as follows.

- A. In the **Credential** section, click the **badge image**.
- B. Select a badge template, and then click **OK**.

Badge templates are created in **Config Tool**. For more information, see the *Security Center Administrator Guide*.

A print preview of the badge appears, with data corresponding to the current cardholder and their credential.

11. Click **Save**.

You must save all your changes before you can print the badge.

12. To print the badge, click **Print badge** next to the badge preview.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 136 of 430

3.7.1.7 Request Credential Cards

When you are not in possession of the credential cards, you can request the credential cards to be assigned to the cardholders you are managing by someone else. You can request a card while you are creating a new cardholder or visitor, or after they are created. In this procedure, it is assumed you have already created a cardholder.

To Request a Credential Card:

1. Do one of the following:
 - For cardholders, open the **Cardholder management** task, select a cardholder, and then Click **Modify** (✎).
2. In the Credential section, click **Add a credential** (+).
3. From the drop-down menu, click **Request card**.
4. In the **Request card** dialog box, select the reason why you are requesting a card.

NOTE: Card request reasons only appear if your administrator has created possible reasons in **Config Tool**.
5. From the **Badge template** drop-down list, select a badge template.

You only need to select a badge template if you want a badge to be printed. Badge templates are created in **Config Tool**. For information, see the *Security Center Administrator Guide*.

A print preview of the badge appears.
6. In the **Activate** option, select when to activate the credential.
 - **Never:** The credential will never be activated.
 - **After enrollment:** After another user responded to the card request.
 - **On:** Select a specific date to activate the credential.
7. If you want to receive an email when the credential has been printed, select the Email me when the card is ready option.

NOTE: For this option to work, your user must have a valid email address.
8. Click **OK**. The credential is shown as **Requested** in the **Credential** section of the cardholder details window.
9. Click **Save**.
10. The **Card requests** (🔔) icon appears in the **notification** tray.

3.7.1.8 Print Paper Credentials

When you do not have credentials assigned to cardholders, you can print paper credentials (badges without credential data) as name tags or photo IDs for visual identification.

To print a badge, you need a badge template. A badge template is generally associated to a card credential so that it can be used to unlock doors, but you can also print a badge without any credential data (called a paper credential) that can be used as a name tag or a photo ID for visual identification.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 137 of 430

You can print a badge while you are creating a new cardholder, or after they are created. It is assumed the cardholder is already created.

For information about creating badge templates, see the *Security Center Administrator Guide*.

To Print a Badge:

1. Do one of the following:
 - For cardholders, open the **Cardholder management** task, select a cardholder, and then click **Modify** (✎).
2. In the **Credential** section, click **Add a credential** (+).
3. In the menu that appears, click **Paper credential** (print).
The **Badge printing** dialog box appears.
4. From the drop-down list, select a badge template.
A print preview of the badge is shown. Cardholder information might be shown on the badge, depending on how the badge template is designed. No credential data is shown on the badge.
5. To print the paper credential, click **Print badge**.

3.7.1.9 Assign Temporary Cards

If a cardholder card credential is reported as lost or stolen, you can replace it with a temporary card and mark the original card as lost.

Make sure that you have the following:

- A card reader nearby.
- A stack of pre-enrolled spare cards. You can enroll a large quantity of cards at once using the **Credential management** task.

To Assign a Temporary Card to a Cardholder:

1. Do one of the following:
 - For cardholders, open the **Cardholder management** task, select a cardholder, and then click **Modify** (✎).
2. In the **Credential** section, click **Assign temporary card**.
3. From the drop-down list, select a card reader near you.
The card reader can be a **USB Reader** connected to your computer, or you can use an **Access point** (door).
4. Present a spare card that is pre-enrolled.
5. Set the number of days the temporary card is to remain active and click **Assign temporary card**.
6. Click **Save**.

After this operation, the original card is marked as **Lost**, but remains assigned to the cardholder. The temporary card is activated for the specified number of days and assigned to the same cardholder. The cardholder now has at least two cards. A permanent one that is lost, and a temporary one that is active.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 138 of 430

3.7.1.10 Restore Original Cards to Cardholders

When a lost card is found, you can restore the original card and remove the temporary card assignment.

Before you begin, make sure you have a card reader nearby.

To restore the original card, the cardholder must return both the original and the temporary card.

- **CAUTION:** When a cardholder has more than one temporary card, returning the temp card restores the original card to the cardholder. The return temporary card functionality can be used only once per cardholder.

To Restore an Original Card to a Cardholder:

1. In the **Cardholder management** task, click **Return card** (🔄).
2. From the drop-down list, select a card reader near you.

The card reader can be a **USB Reader** connected to your computer, or you can use an **Access point** (door).
3. Present both the original and the temporary cards; the order is not important.
4. If both cards match the same cardholder, click **Restore original card** to restore the status of the original card to **Active**, and deactivate the temporary card.

The temporary card can now be assigned to someone else.

3.7.1.11 Signature Pads

If you have a signature pad attached to your computer, you can use it to capture cardholder signatures and save them directly to a signature custom field that was created beforehand.

Make sure cardholder signature custom fields have been created with the Image data type.

Attach a **Topaz signature pad** to your computer and enable it in *Security Desk*.

To Use a Signature Pad:

1. Open the **Cardholder management** task to create or modify the cardholder.
2. In the **property** dialog box, click the custom field reserved for the signature and select **Load from signature pad**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 139 of 430

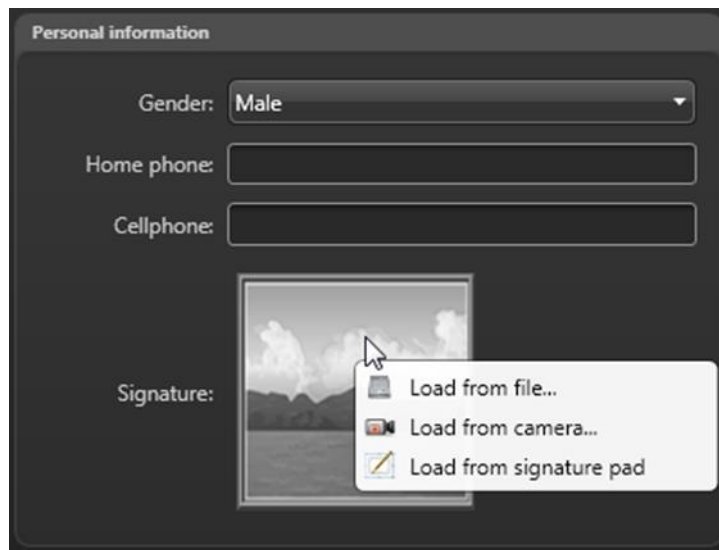


Figure 94. Signature Pad

3. Hand the signature pad to the cardholder and ask them to sign.
The captured signature appears in the signature field.
4. Click **Save**.

3.7.1.12 Investigate Cardholder Events

You can investigate events related to cardholders (Access denied: Invalid PIN, First person in, Last person out, **Antipassback** violation, and so on), using the **Cardholder activities** report.

For example, if you want to see which areas and doors the cardholder has access in the last day or week, you can search for that specific cardholder, and set a time range for your report. If there has been suspicious activity on your site in the last day, you can investigate which cardholders were denied access to an area by selecting the area, and the **Access denied** event.

To Investigate Cardholder Events:

1. From the home page, open the **Cardholder activities** task.
2. Set up the query filters for the report. Choose from one or more of the following filters:
 - **Cardholders:** Restrict the search to certain cardholders.

NOTE: If you only select the **All cardholders** group, federated cardholders are not included. This is because **All cardholders** is a local cardholder group that only covers local cardholders.

 - **Credentials:** Restrict the search to specific credentials.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity and if the custom field was made visible to you when it was created or last configured.
 - **Doors - Areas:** Restrict the search to activities that took place at certain doors and areas.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 140 of 430

- **Events:** Select the events of interest. The event types available depend on the task you are using.
 - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time, such as the previous week or the previous month.
3. Click **Generate report**. The cardholder events are listed in the **report** pane.
 4. Show the corresponding video of an event in a tile by double-clicking or dragging the item from the **report** pane to the canvas. If there is no camera attached to the entity, the door, or area icon is displayed, depending on the type of cardholder event.
 5. Control the tiles using widgets in the dashboard.

3.7.1.13 Report Pane Columns for the Cardholder Activities Task

After generating a report, the results of your query are listed in the **report** pane. This section lists the columns available for the relevant reporting task.

- **Access point:** Access point involved (only applicable to areas and doors).
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity and if the custom fields were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Email address:** Cardholder's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder's last name.
- **Location:** Location (area) where the activity took place.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder's picture.
- **Product type:** Model of the unit involved.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, or intrusion detection unit involved.

3.7.1.14 Count People

You can view the number of cardholders that are currently in secured areas on your system, using the **People counting** task. The number of cardholders present in a selected area is updated in real

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 141 of 430

time as people move in and out of the area.

For the report to be accurate, the selected area must be fully secured, meaning that people should not be allowed to enter or exit the area without swiping their card. Readers should be installed on both sides of a door (no REX's), and cardholders must pass through the door one by one (no tailgating). Turnstiles are often used for this purpose.

To Count the Number of Cardholders in an Area:

1. From the home page, open the **People counting** task.
2. In the **Selector**, select an area. The cardholders present in that area are listed on the right.
3. To launch an investigation report on a selected cardholder, click **Investigate** (🔍).
4. To remove a selected cardholder from the area you are viewing, click **Remove from area** (✖).
5. To reset the people count to zero for the selected area, click **Clear all**.



Figure 95. People Count

The cardholders that you removed using either the **Remove from area** command or the **Clear all** command, are automatically forgiven one antipassback violation the next time they badge their card. This allows them to re-enter the area they have been removed from.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 142 of 430

- **Example:** If you see suspicious activity while monitoring a live video feed, you can use people counting to see cardholders that are currently in that area. If there is a fire in your building, you can use people counting to see if there is anyone left in an area of the building.

3.7.1.15 Track Attendance in an Area

Find out which cardholders have been inside a selected area, and the total duration of their stay within a given date range, using the Time and attendance report.

This report displays the total time spent in the selected area by each selected cardholder for each day covered by the date range. For example, if something happened in an area two days ago, you can find out who was in that area during that day by selecting the area and the date range.

For the report to be accurate, the selected area must be fully secured, meaning that people should not be allowed to enter or exit the area without swiping their card. Readers should be installed on both sides of a door (no REX's), and cardholders must pass through the door one by one (no tailgating). Turnstiles are often used for this purpose.

To Investigate the Duration of a Cardholder's Stay:

1. From the home page, open the **Time and attendance** task.
2. Set up the query filters for the report. Choose from one or more of the following filters:
 - **Areas:** Select the areas to investigate.
 - **NOTE:** You must select a fully secured area.
 - **Cardholders:** Restrict the search to certain cardholders.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
 - **Time range:** The date range for the report.
3. Click **Generate report**.

The total time spent in the selected area by each selected cardholder, for each day covered in the selected date range, are listed in the **report** pane.

3.7.1.16 Track Cardholders Present in an Area

You can see how many cardholders are currently present in a selected area, and how long they have been there, using the Area presence report.

For the report to be accurate, the selected area must be fully secured, meaning that people should not be allowed to enter or exit the area without swiping their card. Readers should be installed on both sides of a door (no REX's), and cardholders must pass through the door one by one (no tailgating). Turnstiles are often used for this purpose.

To Track Which Cardholders are Present in an Area:

1. From the home page, open the **Area presence** task.
2. Set up the query filters for the report. Choose one or more of the following filters:
 - **Areas:** Select the areas to investigate.
 - **NOTE:** You must select a fully secured area.
 - **Cardholders:** Restrict the search to certain cardholders.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 143 of 430

- **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity and if the custom field was made visible to you when it was created or last configured.
3. Click **Generate report**.
The cardholders currently in the selected area are listed in the **report** pane.
 4. To show the corresponding video of an event in a tile, double-click or drag the item from the **report** pane to the canvas.
If the area is not associated to a URL or a map file through a tile plugin, the area icon is displayed.
 5. To control the areas, use the **area** widget.

3.7.1.17 Report Pane Columns for the Area Presence Task

After generating a report, the results of your query are listed in the **report** pane. This section lists the columns available for the relevant reporting task.

- **Area:** Area name.
- **Cardholder:** Cardholder entity name.
- **Cardholder group:** Cardholder groups that the user belongs to.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity and if the custom fields were made visible to you when they were created or last configured.
- **Email address:** Cardholder's email address.
- **First name:** Cardholder's first name.
- **Last access:** Time the cardholder entered the area.
- **Last name:** Cardholder's last name.
- **Picture:** Cardholder's picture.

3.7.1.18 Report Pane Columns for the Time and Attendance Task

After generating a report, the results of your query are listed in the **report** pane. This section lists the columns available for the relevant reporting task.

- **Area:** Area name.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity and if the custom fields were made visible to you when they were created or last configured.
- **Date:** The date.
- **First name:** Cardholder's first name.
- **Last name:** Cardholder's last name.
- **Picture:** Cardholder's picture.
- **Total time:** Total time spent in that area on that date by the cardholder.
- **Weekday:** Weekday corresponding to the date.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 144 of 430

3.7.1.19 View Properties of Cardholder Group Members

You can find out the members of a cardholder group, and view any associated cardholder properties (first name, last name, picture, status, custom properties, and so on) of the cardholders, using the **Cardholder configuration** task.

You can search for a specific cardholder group to see which cardholder is a member of that group. You also can search for expired or inactive cardholders to see if there are any in your system.

To View the Properties of Cardholder Group Members:

- From the home page, open the **Cardholder configuration** task.
- Set up the query filters for your report. Choose one or more of the following filters:
 - Activation date:** Time the cardholder's profile was activated.
 - Expiration date:** Specify a time range for when the cardholder's profile expired.
 - Unused cardholders:** Search for cardholder for whom no assigned credentials have produced an access granted event within a certain time range.
 - NOTE:** For the report to generate results, all **Access Manager** roles must be active and online.
 - Status:** The status of the cardholder's profile: **Active; Expired; Inactive; Lost; Stolen**. Not all statuses are available for every task.
 - First name:** Cardholder's first name.
 - Last name:** Cardholder's last name.
 - Email address:** Cardholder's email address.
 - Description:** Restrict the search to entries that contain this text string.
 - Picture:** Cardholder's picture.
 - Partition:** Partition that the entity is a member of.
 - Cardholder groups:** Restrict the search to specific cardholder groups.
 - Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity and if the custom field was made visible to you when it was created or last configured.
 - Credentials:** Restrict the search to specific credentials.
 - Credential status:** The status of the cardholder's credential: **Active; Expired; Inactive; Lost; Stolen**. Not all statuses are available for every task.
 - Credential information:** Restrict the search to specific card formats, facility codes, or card numbers.
- Click **Generate report**. The cardholders that are members of the selected cardholder groups are listed in the **report** pane.
- To show a cardholder in a tile, double-click or drag a cardholder from the **report** pane to the canvas.
- To view additional cardholder information in the tile, click .

3.7.1.20 Report Pane Columns for the Cardholder Configuration Task

After generating a report, the results of your query are listed in the **report** pane. This section lists the columns available for the relevant reporting task.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 145 of 430

- **Cardholder:** Cardholder entity name.
- **Cardholder activation date:** Date that the cardholder's profile was activated.
- **Cardholder expiration date:** Date that the cardholder's profile expires.
- **Cardholder status:** The cardholder's profile status.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity and if the custom fields were made visible to you when they were created or last configured.
- **Email address:** Cardholder's email address.
- **First name:** Cardholder's first name.
- **Last name:** Cardholder's last name.
- **Member of:** All groups the cardholder belongs to.
- **Picture:** Cardholder's picture.

3.7.1.21 Modify Cardholder Dialog Box

Once you have created a cardholder, you can always go back and modify their properties, credentials, and access rights, by selecting the cardholder in the **Cardholder management** task, and then clicking **Modify** (✎).

The properties you can edit depend on your user privileges. [Figure 96](#) shows the **cardholder modification** dialog box.

Figure 96. Cardholder Modification Dialog Box

A. Cardholder's basic properties

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 146 of 430

- B. Edit the cardholder's picture
- C. To remove the cardholder's picture, right-click, and then click **Clear the picture**
- D. Assign additional access rights to the cardholder from the **Access rules** tab
- E. Additional cardholder information
- F. Edit the cardholder's credential
- G. Remove the cardholder's credential
- H. Switch between cardholders
- I. Save or cancel your changes.
- J. Icons
 -  – Report on the cardholder
 -  – Report on the cardholder's credential
 -  – Report on the changes made to the cardholder

3.7.1.22 Search for Cardholders

If you have a large access control system and cannot find a cardholder, you can search for them by name, or use the advanced search by applying a combination of filters.

To Search for a Cardholder:

1. From the home page, do one of the following:
 - Open the **Cardholder management** task.
2. To search by an entity name, type the name in the **Search**  box.
All entities with names that match the text you entered are listed.
3. To search for the entity using the advanced search:
 - A. In the left pane, click **Advanced search**.
 - B. Set up the query filters for the report. Not all query filters are available for each task. Choose from one or more of the following, according to your task:
 - **Activation date:** Time the cardholder's profile was activated.
 - **Expiration date:** Specify a time range for when the cardholder's profile expired.
 - **Unused cardholders:** Search for cardholders for whom no assigned credentials have produced an access granted event within a certain time range.

NOTE: For the report to generate results, all Access Manager roles must be active and online.

 - **Status:** The status of the cardholder's profile: **Active**; **Expired**; **Inactive**; **Lost**; **Stolen**. Not all statuses are available for every task.
 - **First name:** Cardholder's first name.
 - **Last name:** Cardholder's last name.
 - **Email address:** Cardholder's email address.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 147 of 430

- **Description:** Restrict the search to entries that contain this text string.
- **Picture:** Cardholder's picture.
- **Partition:** Partition that the entity is a member of.
- **Cardholder groups:** Restrict the search to specific cardholder groups.
- **Credentials:** Restrict the search to specific credentials.
- **Credential status:** The status of the cardholder's credential: **Active; Expired; Inactive; Lost; Stolen.** Not all statuses are available for every task.
- **Credential information:** Restrict the search to specific card formats, facility codes, or card numbers.
- **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity and if the custom field was made visible to you when it was created or last configured.
- **Escort required:** Specify that an escort is required.

C. Click **Search**.

The cardholders or visitors that match your search criteria are displayed on screen.

- **Example:** Let's assume that the cardholder or visitor you are searching for has a card that was activated less than a week ago. In the **Activation date filter**, enter 7 days in the **During the last** box.

3.7.1.23 Report Pane Columns for Cardholder Management Tasks

After generating a report, the results of your query are listed in the **report** pane. This section lists the columns available for the relevant reporting task.

NOTE: Not all **report** pane columns are available for both the Cardholder management task and the Visitor management task.

- **Activation date:** Time the cardholder or visitor's profile was activated.
- **Cardholder:** Cardholder entity name.
- **Cardholder status:** The cardholder's profile status.
- **Check-in date:** Time the visitor was checked in (can correspond to the arrival time).
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity and if the custom fields were made visible to you when they were created or last configured.
- **Description:** Description of the event, activity, entity, or incident.
- **Email address:** Cardholder or visitor's email address.
- **Escort required:** Indicates whether an escort is required.
- **Expiration date:** Time the cardholder or visitor's profile expired.
- **First name:** Cardholder or visitor's first name.
- **Last access:** Time and details of the last access event involving the cardholder or the credential.
- **Last name:** Cardholder or visitor's last name.
- **Member of:** All groups the cardholder belongs to.
- **Picture:** Cardholder or visitor's picture.
- **Role:** Role type that manages the selected Federated or Active Directory imported entity.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 148 of 430

- **Security clearance:** The cardholder's security clearance level.
- **Status:** The visitor's profile status.
- **Visitor host:** The visitor's host (or escort).

3.7.1.24 Search for Cardholders and Visitors Using Credentials

If you have an unidentifiable card, you can find the cardholder or visitor it belongs to by presenting the card at a USB reader or door.

Make sure that you have a USB reader connected to your computer, or that there is a door you can present the card at.

To search for a cardholder or visitor by using their credential:

1. From the home page, click **Cardholder management**.
2. At the top of the **task** window, click .
3. From the drop-down list in the **search** window, select one of the following:
 - **USB Reader:** A USB reader that is connected to your computer.
 - **Door:** An access point close by.
4. Present the card to the device selected in the previous step.

If the card is assigned to a cardholder or visitor, the **search** dialog box closes, and the corresponding person is selected in the cardholder or visitor list. If the card is not assigned to a cardholder or visitor, the reason that the card is rejected is displayed in the **search** dialog box. You can present another card or click **Cancel** to stop the operation.

- **Example:** If you found a card in the office or parking lot and it has no name or picture on it, you can identify who it belongs to.

3.7.2 Cardholder Groups

A cardholder group is a type of entity that configures the common access rights of a group of cardholders. If you have a large access control system, cardholders and access rules are much easier to manage when cardholders are members of cardholder groups.



Figure 97. Cardholder Groups

- Assigning Cardholder Groups to Access Rules is recommended.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 149 of 430

- Cardholders can belong to multiple cardholder groups.
- Cardholders inherit access by belonging to groups linked to access rules.

3.7.2.1 Create a Cardholder Group

To configure the access rights and properties that are common to a group of cardholders, you can create cardholder groups. If you have a large access control system, cardholders and access rules are much easier to manage when cardholders are members of cardholder groups.

To Create a Cardholder Group:

1. Open the **Access control** task and click the **Cardholder groups** view.
2. Click **Cardholder group**. A new cardholder group appears in the entity tree.
3. Type a name for the group, and press **ENTER**.
4. Select the cardholder group, click the **Properties** tab.
5. At the bottom of the page, click  to add individual cardholders or cardholder groups to your new group.
6. Click **Apply**.

3.7.3 Receive Notifications When Cardholders Are Expiring

You can configure Security Center to send you or another user an email before cardholders or their credentials expire. If you want the user to be notified by email, make sure they have a valid email address.

Users can be notified for every cardholder or credential that is expiring soon, or only for specific entities. If a cardholder expires, their credential is no longer valid.

To Receive a Notification When a Cardholder or their Credential is Expiring:

1. Open the **Access control** task and click the **General settings** view.
2. Switch the **'Trigger event 'Entity is expiring soon'** option to **ON** and select how many days prior to the expiration to trigger the event.
3. Click **Apply**.
4. Open the **System** task and click the **General settings** view.
5. Click **Actions**, then click **Add an item** .
6. In the **Event-to-action** page, scroll down the **When** list and click **Entity is expiring soon**.
7. (optional) Select an entity in the **From** list.
 - **CAUTION:** Make sure that the entity you select is the one you want to monitor. If you select a cardholder, and it is the credential that is expiring soon, the event-to-action will not be executed.
8. Under the **Action** menu, select **Send an email**, then select the **Recipients**, edit the email, and set the **Priority**.
9. Click **Save**.
10. If necessary, change the time range when this **event-to-action** is in effect.
11. The recipient is sent an email the specified number of days before the entity expires.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 150 of 430

Figure 98. Event to Action

3.8 CREDENTIALS

Credentials means any user name, identification number, password, license, security key, security token, PIN or other security code, method, technology or device used, alone or in combination, to verify an individual's identity and authorization to access and use the Hosted Services.

3.8.1 Credential Management

To control access to sensitive areas such as doors and data, organizations require user credentials. Deploying a sound credential management system, or several credential management systems is critical to secure all areas systems and information. Authorities must be able to create and revoke credentials as visitors and employees come and go or simply change roles, and as business processes and policies evolve. Furthermore, the rise of privacy regulations and other security mandates increases the need for organizations to demonstrate the ability to validate the identity of workers, consumers, visitors and internal privileged users.

3.8.2 Credentials – Access Control Task

Cardholders and credentials tab displays:

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 151 of 430

- Partition
- Cardholder group
- Cardholder
- Credential

Credentials can be created, deleted or modified here.

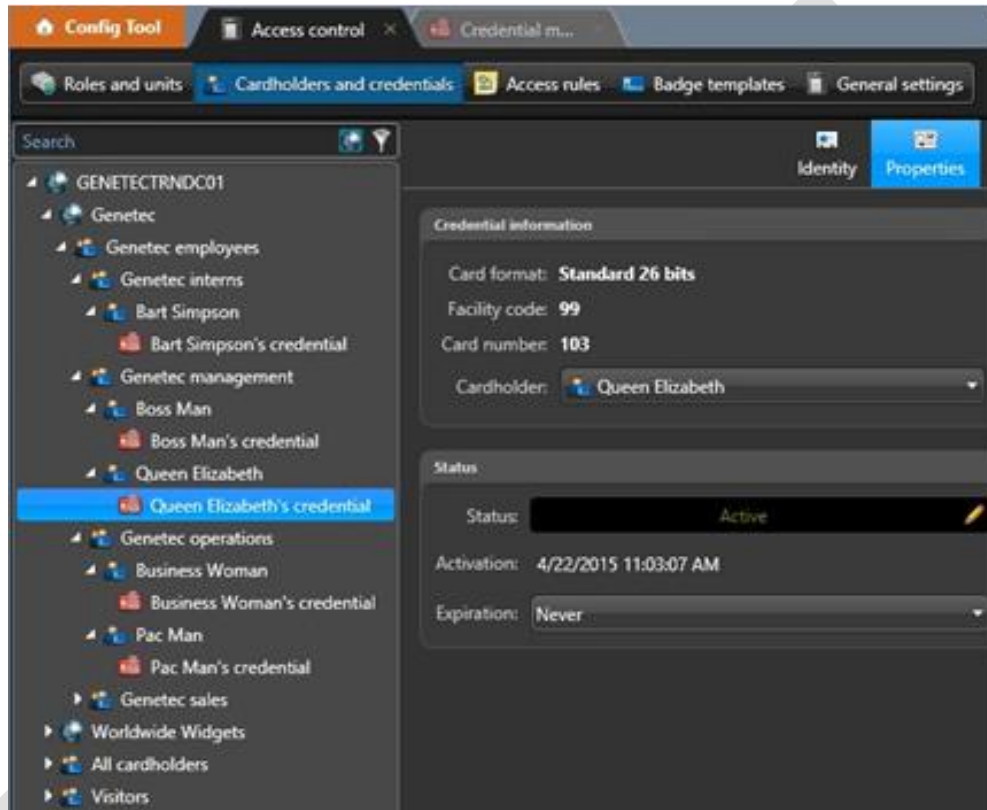


Figure 99. Credentials: Access Control Task

3.8.3 Credentials – Access Management Task

The credential management task displays a flat list showing:

- Cardholder
- Picture
- Cardholder group
- Last access

Credentials can be created, deleted, modified here.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 152 of 430



Figure 100: Credentials: Access Management Task

3.8.4 Unused Credential and Cardholder Expiration Field

The **Expiration** field is included in a cardholder entity name

- Typically referred to as the “use it or lose it” rule
- Cardholder or credential property
- Keeps from having unused cardholders and credentials cluttering the system
- Requires Security Center 5.5 minimally
- Supports Synergis and HID controllers

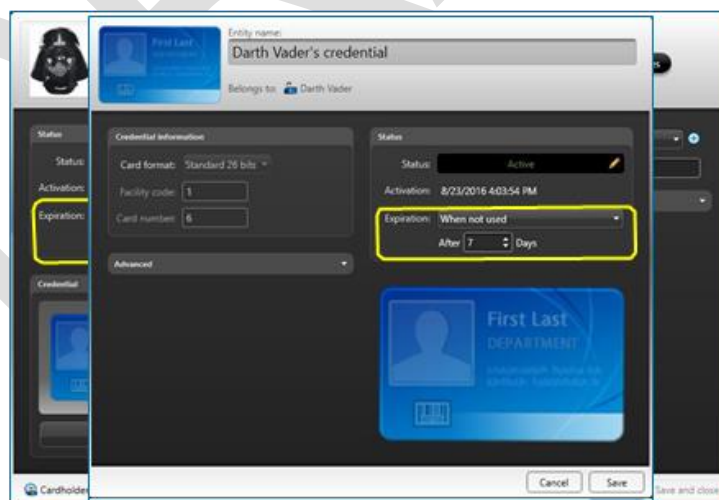


Figure 101. Credentials: Unused Credential & Cardholder Expiration

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 153 of 430	

3.8.5 Search Unused Credentials and Cardholders

You can search credentials that will be expiring soon from the **Credential Management** task, and which cardholders or visitors have already expired from the **Cardholder** or **Visitor Management** tasks.

- Expiration setup can be copied to other entities using the **Copy Configuration** tool
- Expiration is only enforced if the unit is online to receive the request
- Can also search by “**Unused Credential**”

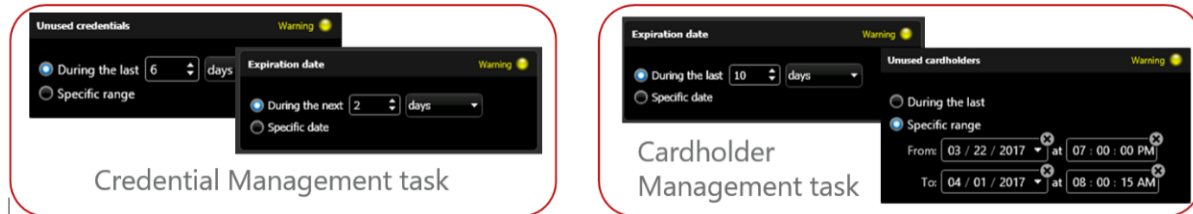


Figure 102. Credentials: Search Unused Credentials and Cardholders

3.8.6 Credential Access Control

Figure 103 shows the Credential Access Control tab displays:

- Credential
- Credential Status
- Cardholder
- Cardholder group
- Credential Code
- Last Access Time

Credential	Credential status	Cardholder	Picture	Card format	Credential code	Last access time
88uiuu oiouio's credential	Inactive	Jay Bautista		Unknown 36 bits		Unknown
Aaron Full's credential	Active	Aaron Full		HID Corporate 1000 35 Bits	1646/249006	1/20/2020 2:23:31 PM
Alex Hussey's credential	Inactive	Alex Hussey		Standard 26 bits	14/25428	12/19/2019 12:26:00 PM
Anthony Garcia's credential	Inactive	Anthony Garcia		Unknown 36 bits		Unknown
Arnold Dicion's credential	Active	Arnold Dicion		Unknown 36 bits		Unknown
Brandon Reisen's credential	Active	Brandon Reisen		Unknown 36 bits		Unknown
Ceriaco Belza	Inactive	Ceriaco Belza		Standard 26 bits	14/25424	1/7/2020 1:58:46 PM
Dan McColloch's credential	Active	Dan McColloch		Standard 26 bits	14/25491	1/15/2020 7:37:26 AM
Danny McNamee's credential	Active	Danny McNamee		Standard 26 bits	21/35	1/20/2020 9:32:01 AM

Figure 103. Access Control Configuration: Credential Management

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 154 of 430	

As shown in [Figure 104](#) Credentials can be created, deleted, or modified here.

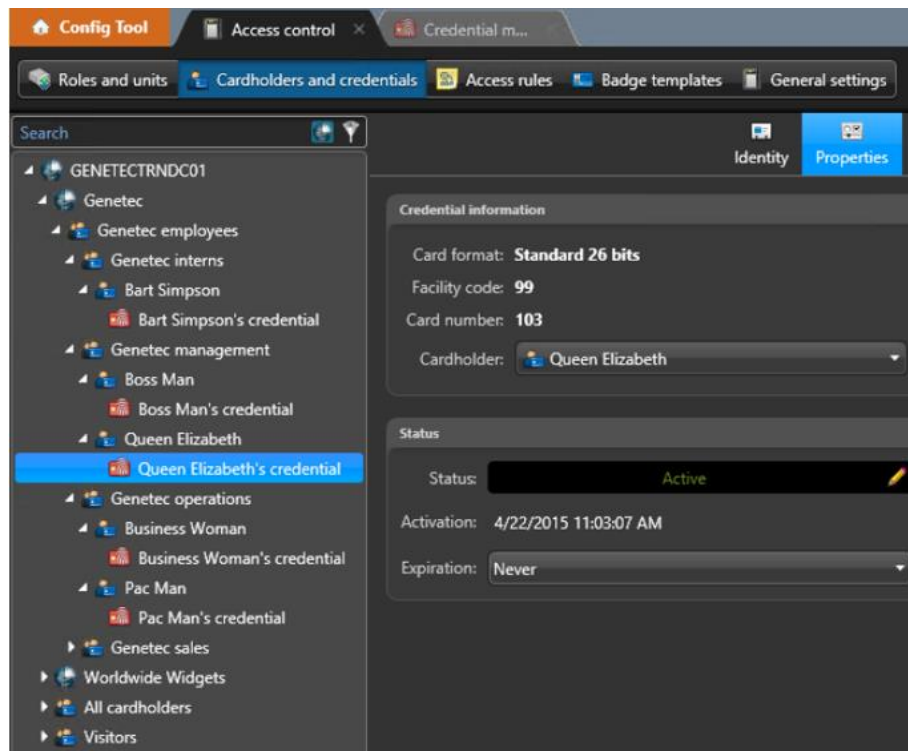


Figure 104. Cardholders and Credentials

3.8.7 Credential Management Task

Use the **Credential management** task to create, modify, and delete credentials, and print badges. The following figure shows the **Credential management** task.

- **NOTE:** You can only have one instance of this task in Security Desk.

The letters below correspond to those in [Figure 105](#).

- View, modify, or respond to outstanding credential card requests.
- Find a credential by name.
- Advanced search options.
- Select which columns to display by right-clicking the column headers or by typing **CTRL+SHIFT+C**.
- Switch between **Tiles** and **List** view.
 - **Tiles:** Shows large pictures. Pictures can be resized.
 - **List:** List all information concerning the entity: first name, last name, picture, activation date, expiration date, check-in date, and any custom fields that are defined.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 155 of 430

- F. Enroll multiple credentials into your system at once.
- G. Print the selected credential cards.
- H. View or modify the selected credential.
- I. Delete the selected credentials.
- J. Create a new credential.

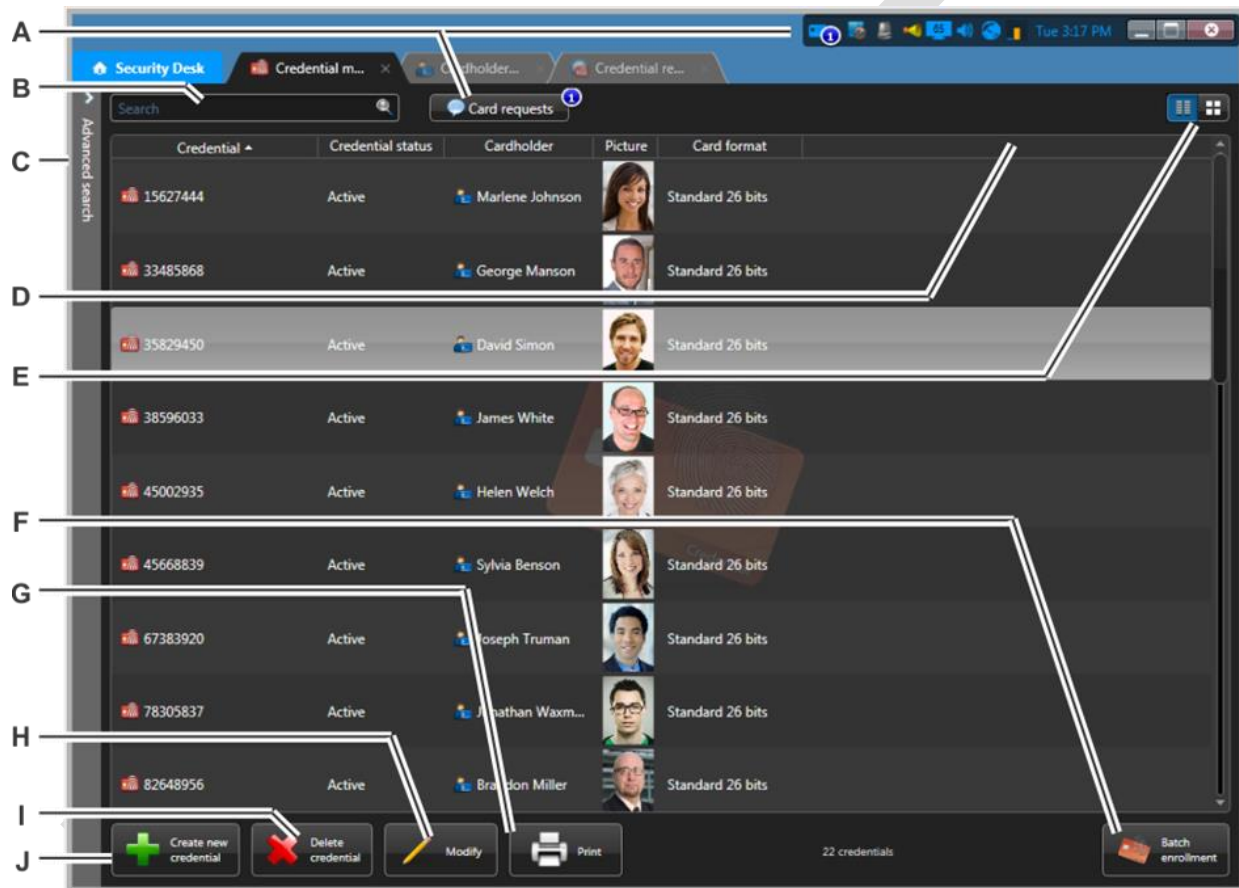


Figure 105. Credential Management Task

3.8.8 Credential Enrollment Methods

If you need many card credentials in your access control system, you can enroll multiple credentials at a time.

The following two enrollment methods are available in the **Credential management** task:

Automatic entry: This is the recommended method when the cards you want to enroll are at your disposal, and when the card data is not found within any known range of values. It is also appropriate to use this enrollment method when the cards come in many types of formats.

Manual entry: This is the recommended method when all the cards you want to enroll are the

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 156 of 430	

same format, and one of the data fields (typically the Card number) contains a range of consecutive values. You do not require the actual cards, or a card reader to use this method, and it can be an effective way of pre-enrolling large quantities of cards.

You can also enroll credentials using the Import tool. For more information about importing credentials using the **Import** tool, see the *Security Center Administrator Guide*.

3.8.9 Enroll Credentials Multiple Automatically

If you need many card credentials in your access control system, you can enroll multiple card credentials automatically by presenting them to a reader.

You must have access to a card reader. The cards you present must be from a predefined format in your system. Make sure that this is the correct enrollment method you require.

All credentials you enroll must be new to your *Security Center* system. Any previously enrolled credential is discarded, because the same credential cannot be enrolled twice in ***Security Center***.

To enroll multiple credentials automatically:

1. In the **Credential management** task, click **Batch enrollment**.
2. In the **Automatic entry** tab, select a card reader that is nearby.
Ensure the selected reader supports the card formats you have.
3. In the **Credential prefix** section, type the pattern for the enrolled credential names.
4. In the **Credential status** section, set the **status**, **activation date**, and **expiration date** for the credentials.
 - **Status:** All possible values are accepted.
 - **Activation:** Can be Never, or a specific date.
 - **Expiration:** Set an expiration for the credential:
 - **Never:** The credential never expires.
 - **Specific date:** The credential expires on a specific date and time.
 - **Set expiration on first use:** The credential expires after a specified number of days after the first use.
 - **When not used:** The credential expires when it has not been used for a specified number of days.
5. In the **Security** section, select the partition the enrolled credentials belong to.
This field determines which users can view and modify the credentials.
 - To add a partition, click **Add** (+).
 - To remove a partition, select the partition, and then click **Remove** (X).
6. From the Badge template drop-down list, select the default badge template used to represent the credential.
7. In the **Custom fields** section, set the default values for the custom fields.
8. Custom fields are only available if they have been created for credentials.
9. Present the cards on the selected reader.

All presented cards are listed in the **Generated credentials** section.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 157 of 430

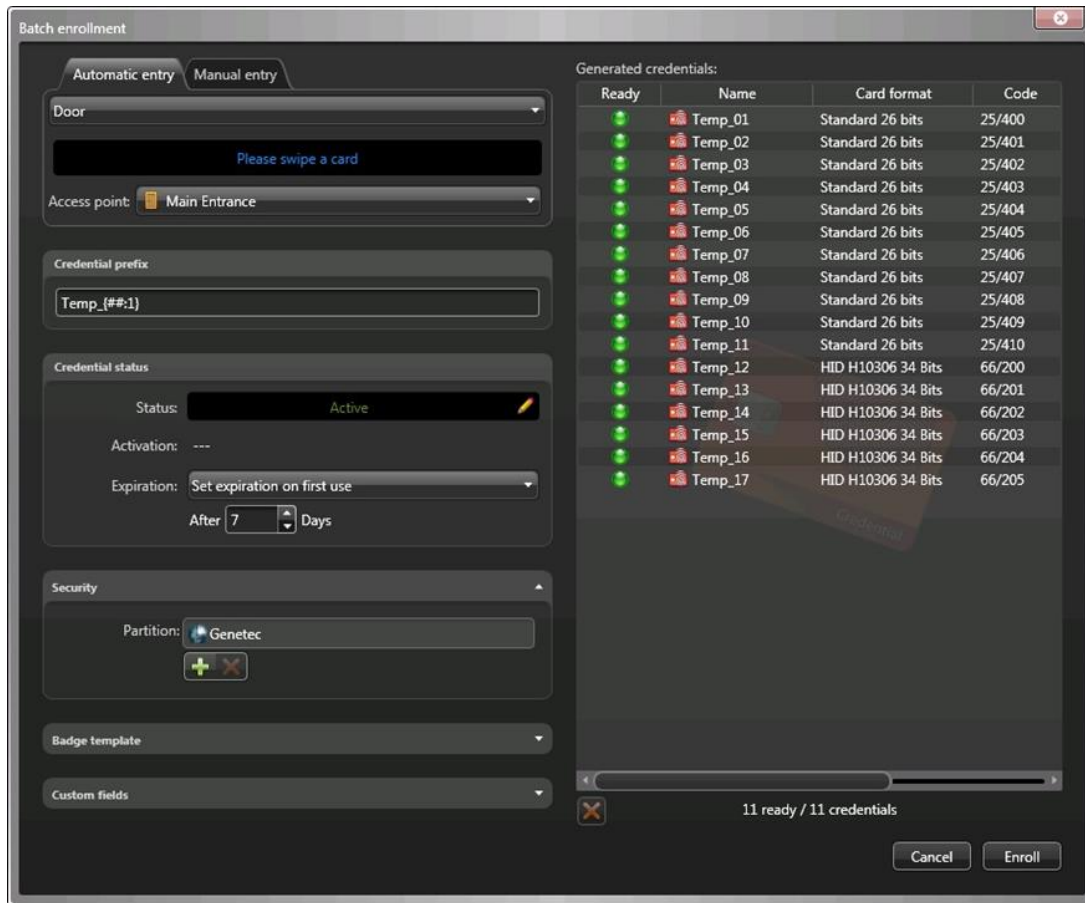


Figure 106. Batch Enrollment: Automatic Credentials

If some of the credentials are already enrolled, they are discarded, and marked as rejected in the list with a red button. If you present the same card twice, it is highlighted momentarily in the list.

1. To remove a discarded card from the list, select it, and click (✗).
2. Click **Enroll**.
3. After you finish assign the credentials to your cardholders.

3.8.10 Enroll Multiple Credentials Manually

If you need many card credentials in your access control system, you can enroll multiple credentials simultaneously by entering the card format and data manually.

Before you begin

You must know the exact range of values represented in the card data. Because those cards are not presented by a reader, the application cannot validate them.

Make sure that this is the correct enrollment method you require.

All credentials you enroll must be new to your *Security Center* system. Any previously enrolled credential is discarded, because the same credential cannot be enrolled twice in *Security Center*.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 158 of 430

Only a maximum of 5000 credentials can be created at once.

To Enroll Multiple Credentials Manually:

1. In the **Credential management** task, click **Batch enrollment**.
2. Click the **Manual entry** tab.
3. From the **Card format** drop-down list, set the card format used by the credentials you want to enroll.

This option determines the data fields you must enter, and the range of values that they can have.

4. In the **Facility code** and **Card number** fields, enter the starting and ending values for the card numbers.
 - The **Card number** field is used as a sequence generator.
 - **NOTE:** If the specified Card number range contains more than 5000 values, the end value is automatically adjusted to be the start value plus 5000.
5. In the **Credential prefix** section, type the pattern for the enrolled credential names.
6. In the **Credential status** section, set the status, activation date, and expiration date for the credentials.
 - **Status:** All possible values are accepted.
 - **Activation:** Can be Never, or a specific date.
 - **Expiration:** Set an expiration for the credential:
 - **Never:** The credential never expires.
 - **Specific date:** The credential expires on a specific date and time.
 - **Set expiration on first use:** The credential expires after a specified number of days after the first use.
 - **When not used:** The credential expires when it has not been used for a specified number of days.

7. In the **Security** section, select the partition the enrolled credentials belong to.

This field determines which users can view and modify the credentials.

- To add a partition, click **Add** (+).
 - To remove a partition, select the partition, and then click **Remove** (X).
8. From the **Badge template** drop-down list, select the default badge template used to represent the credential.
 9. In the **Custom fields** section, set the default values for the custom fields.
 10. Custom fields are only available if they have been created for credentials.
 11. Click **Enroll**.

The credentials you are going to create are listed in the **Generated credentials** section.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 159 of 430

Figure 107. Batch Enrollment: Manual Credentials

If some of the credentials are already enrolled, they are discarded, and marked as rejected in the list with a red button.

12. To remove a discarded credential from the list, select it, and then click (X).
13. Click **Enroll**.
14. After you finish assign the credentials to your cardholders.

3.8.11 Create Credentials

You can create a new credential, configure its properties, and assign it to a cardholder or visitor, using the **Credential management** task.

Instead of creating credentials manually, you can import them from a **CSV** file, or from your company's **Active Directory**. For more information, see the *Security Center Administrator Guide*).

To Create a Credential:

1. In the **Credential management** task, click **Create new credential** (+).
2. Select one of the following options:
 - **Automatic entry**: Present the card at a reader.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 160 of 430

- **Manual entry:** Manually enter the card data. Use this method when you do not have a card reader near you.
 - **PIN:** Create a PIN credential.
3. If you select **Automatic entry**, you must then select a reader (USB reader or a door) and present the card at the reader.

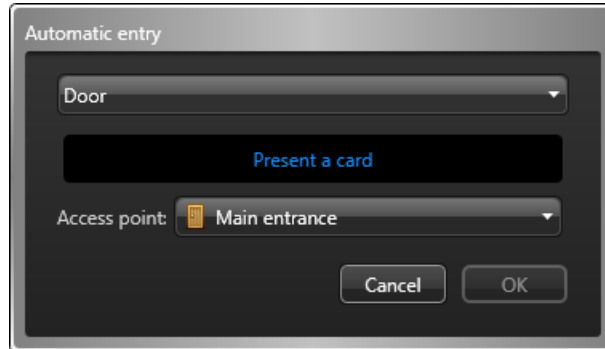


Figure 108. Create Credentials: Automatic Entry - Door

4. If you have a smart card encoding reader set up, set the option **Encode** before enrollment to **OFF** to read a pre-encoded card.

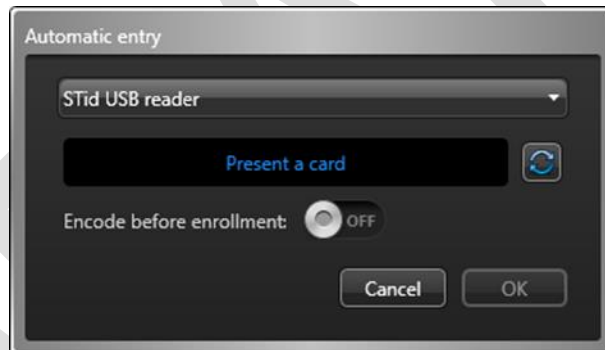


Figure 109. Create Credentials: Automatic Entry - Encode OFF

When the reader LED turns green (ready to read), place the smart card on the reader. The reader LED turns yellow and then green with a short beep before turning off.

If you want to generate and encode on your card a random 128-bit DESFire EV1 credential before enrolling it, set the option **Encode** before enrollment to **ON**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 161 of 430

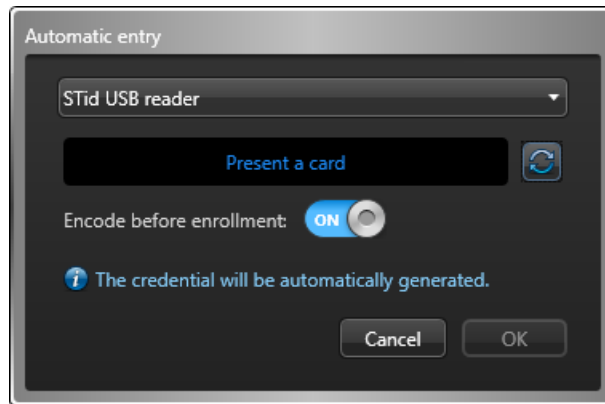


Figure 110. Create Credentials: Automatic Entry - Encode ON

When the reader LED turns red (ready to encode), place the smart card on the reader for approximately 2 seconds. The reader LED turns yellow and then green with a short beep before turning off. If you hear a long beep and the LED stays red, try again.

5. If you select **Manual entry**, you must then select a card format, enter the required data fields, and click **OK**.

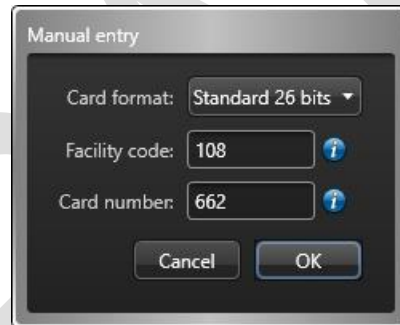


Figure 111. Create Credentials: Manual Entry

CAUTION: Enter your card data carefully, because the system cannot validate whether the data you entered correspond to a physical card or not.

6. If you select **PIN**, you must then do the following:

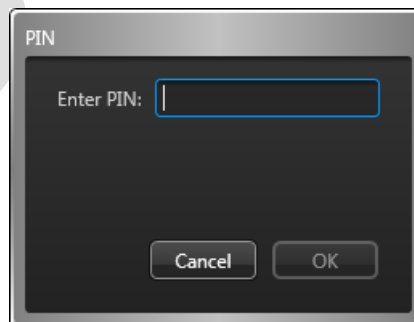


Figure 112. Create Credentials: Manual Entry: PIN

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 162 of 430

- A. Enter the **PIN** as a numerical value.
- B. **NOTE:** Be careful not to exceed the number of digits accepted by your readers. A typical **PIN** length is five digits. But certain models accept up to 15 digits.
- C. Click **OK**.

7. In the **Entity name** field, enter a name for the credential entity.

The following screenshot is for card credentials. The dialog box looks different if you selected **PIN** or another credential type.

The screenshot shows a 'Create Credentials' dialog box. At the top, there's a header with a user icon and 'Entity name: New credential'. Below that, 'Belongs to: Unassigned (click to assign)'. The main area is divided into sections: 'Credential information' with 'Card format: Standard 26 bits', 'Facility code: 223', and 'Card number: 3446'; 'Status' with 'Status: Active', 'Activation: 07/02/2017 5:48:29 PM', and 'Expiration: Never'; 'Card details' with 'Manufacturer: HID' and 'Model: ProxiCard II'; and 'Advanced' with 'Description' and 'Partition: TW-SC-5'. On the right, there's a preview of the credential card showing a person's photo, the Genetec logo, and a barcode. At the bottom, there are 'Print badge', 'Cancel', and 'Save' buttons.

Figure 113. Create Credentials: Manual Entry - Entity Name

8. Click the **Belong to** field, select a cardholder or visitor to assign the credential to, and then click **OK**. Without assigning a credential, you cannot monitor the activities, or generate activity reports for that cardholder or visitor.
9. In the **Status** section, set the status and activation period for the credential.

If the credential is inactive, the cardholder or visitor does not have access to any area.

- **Status:** Set the credential status to Active.
- **Activation:** Displays the current date.
- **Expiration:** Set an expiration for the credential:
 - **Never:** The credential never expires.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 163 of 430

- **Specific date:** The credential expires on a specific date and time.
 - **Set expiration on first use:** The credential expires after a specified number of days after the first use.
 - **When not used:** The credential expires when it has not been used for a specified number of days.
10. If custom fields are defined for credentials, such as the manufacturer, the card model, and so on, enter the credential's custom information under the designated section.
 11. Optional: Click the **Advanced** section, and configure the following credential properties:
 - A. In the **Description** field, type a description for the credential.
 - B. Assign the credential to a partition.
Partitions determine which *Security Center* users have access to this entity. Only accepted users of the partition can view or modify the credential.
 12. Optional: If the credential is a card credential (not a PIN), select a **badge** template.
 - A. In the lower-right corner of the **credential details** dialog box, click the **badge image**.
 - B. Select a **badge** template, and then click **OK**.
 - **Badge templates** are created in **Config Tool**. For information, see the *Security Center Administrator Guide*.
 - A print preview of the badge appears, with data corresponding to the credential.
 - **NOTE:** The badge template remains associated to the credential even if you unassign the credential from a cardholder or visitor.
 13. To print the badge, in the lower-left corner of the **credential details** dialog box, click **Print badge**.
 14. When you are finished editing the credential, click **Save**.
 15. The new credential is added to the list in the **Credential management** task.

After you finish to modify a credential, select the **credential** in the list, and then click **Modify** (✎).

3.8.12 Respond to Credential Card Request

After a credential card request has been made, you can respond by assigning a credential to the applicant the request was made for, or by denying the request.

The number of pending card requests is shown in the **Card requests** (🔔) icon in the notification tray, and at the top of the Credential management task.

Credential requests are sent when a user creates a new cardholder but cannot assign a credential or print a card for the cardholder (for example, because no printer is available). After you assign and print a credential card, it can be shipped to another site, if required.

To Respond to a Credential Card Request:

1. Do one of the following:
 - In the notification tray, click **Card requests** (🔔).
 - At the top of the **Credential management** task, click **Card requests**.
2. In the **Card requests** dialog box, select the request you want to respond to.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 164 of 430

Hold **SHIFT** to select multiple requests.

3. To modify the request, click **Modify** (✎), edit the request, and then click **OK**.
4. To deny the request, click **Deny request** (🚫).
5. To assign a card credential, click **Associate card** (📇).
6. In the **Associate cards** dialog box that opens, do one of the following:
 - To assign a credential automatically, click **Automatic entry**, then select a reader (USB reader or a door), and present the card at the reader.
 - If an eligible card is presented, it is immediately assigned. If the card has not been enrolled, it is enrolled automatically. If the card was already assigned to someone, it is rejected.
 - To assign a credential manually, click **Manual entry**, then select a card format, enter the required data fields, and click **Enroll**.
 - If an eligible card is entered, it is immediately assigned. If the card has not been enrolled, it is enrolled automatically. If the card was already assigned to someone, it is rejected.
 - **CAUTION:** Enter your card data carefully, because the system cannot validate whether the data you entered correspond to a physical card or not.
 - To assign an existing credential, click **Existing credential**, then double-click a **credential** from the list of eligible credentials.
7. To print the badge on the card, click **Print cards** (🖨) and follow the instructions.
8. Click **Close** to complete this request.

After the card request is completed or denied, an email is sent to the requester only if they selected the Email me when the card is ready option when they requested the card.

3.8.13 Investigate Request History of Credential Card

You can see which users requested, cancelled, and printed credential cards, using the Credential request history report.

Before you begin

To receive results in the Credential request history report, you must already be monitoring credential request user activities. For information about how to select which activities to monitor and record in the database from the System task in **Config Tool**, see the *Security Center Administrator Guide*.

Credential badges are usually requested if there is no printer located on the site. If you create a report of the badges that were printed in the last month, the report results can be used as billing information.

To Investigate the Request History of Credential Badges:

1. From the home page, open the **Credential request history** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
 - **Activities:** Select which badge printing activities to investigate.
 - **Credential request:** When a user requests a badge printing job.
 - **Credential request cancelled:** When a user cancels a badge printing job.
 - **Credential request completed:** When a user prints a badge from the queue.
 - **Cardholders:** Restrict the search to certain cardholders.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 165 of 430

- **Credentials:** Restrict the search to specific credentials.
- **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
- **Printing users:** Restrict the search to specific users that printed a badge.
- **Requesting users:** Restrict the search to specific users that requested to print a badge.

3. Click **Generate report**.

The credential badge printing events are listed in the **report** pane.

3.8.14 Report Pane Columns for the Credential Request History Task

After generating a report, the results of your query are listed in the **report** pane. This section lists the columns available for the relevant reporting task.

- **Activity name:** Type of activity.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Credential:** Credential name used by the cardholder.
- **Date/time queued:** The date and time that the badge printing job was requested
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **Request reason:** Reason why the new credential was requested.
- **Requester email:** Email address of the user who requested the badge printing job.
- **User:** Name of the user who triggered the event. The user name is empty if the event was not triggered from *Security Desk*.

3.8.15 Investigate Credential Events

You can investigate events related to credentials (**Access denied: Expired credential**, **Access denied: Inactive credential**, **Access denied: Stolen credential**, and so on), using the **Credential activities** report.

In the **Credential activities**, you can investigate areas a cardholder accessed by selecting the credential, and the time range. You also can search by critical credential events. For example, if an **Access denied: Stolen credential** event occurred, you can see who tried to use the stolen credential by reviewing the video associated with the event.

To Investigate Credential Events:

1. From the home page, open the **Credential activities** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
 - **Credentials:** Restrict the search to specific credentials.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
 - **Doors - Areas:** Restrict the search to activities that took place at certain doors and areas.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 166 of 430

- **Events:** Select the events of interest. The event types available depend on the task you are using.
 - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the previous week or the previous month.
3. Click **Generate report**. The credential events are listed in the **report** pane.
 4. To show the corresponding video of an event in a tile, double-click or drag the item from the **report** pane to the canvas.

If there is no camera attached to the entity, the door, or area icon is displayed, depending on the type of credential event.

5. To control the tiles, use the widgets in the dashboard.

3.8.16 Report Pane Columns for the Credential Activities Task

After generating a report, the results of your query are listed in the **report** pane. This section lists the columns available for the relevant reporting task.

- **Access point:** Access point involved (only applicable to areas and doors).
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Email address:** Cardholder or visitor's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder or visitor's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Location:** Location (area) where the activity took place.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, intrusion detection unit involved.

3.8.17 View Credential Properties of Cardholders

You can view credential properties (**status**, **assigned cardholder**, **card format**, **credential code**, **custom properties**, and so on) of cardholders, using the **Credential configuration** report.

For example, the Credential configuration report is helpful if you requested a credential for a

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 167 of 430

cardholder and want to see if it was activated. If you search by cardholder, the **Credential status** column indicates whether the credential is in the Requested or Active state. You can also search if there are any credentials currently listed as lost or stolen.

To View the Credential Properties of a Cardholder:

1. Open the **Credential configuration** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
 - **Credential:** Specify whether or not the credential is assigned.
 - **Cardholders:** Restrict the search to certain cardholders.
 - **Credential information:** Restrict the search to specific card formats, facility codes, or card numbers.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
 - **Status:** The status of the cardholder or visitor's profile: **Active; Expired; Inactive; Lost; Stolen.** Not all statuses are available for every task.
 - **Unused credentials:** Search for credentials that have not produced an access granted event within a certain time range.
 - **NOTE:** For the report to generate results, all Access Manager roles must be active and online.
3. Click **Generate report**. The credential properties the selected cardholder are listed in the **report** pane.
4. To show a cardholder in a tile, double-click or drag a cardholder from the **report** pane to the canvas.
5. To view additional cardholder information in the tile, click (i).

3.8.18 Report Pane Columns for the Credential Configuration Task

After generating a report, the results of your query are listed in the **Report** pane. This section lists the columns available for the relevant reporting task.

- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Cardholder activation date:** Date that the cardholder's profile was activated.
- **Cardholder expiration date:** Date that the cardholder's profile expires.
- **Cardholder status:** The cardholder's profile status.
- **Credential:** Credential name used by the cardholder.
- **Credential activation date:** Time the cardholder's credential was activated.
- **Credential code:** Facility code and card number.
- **Credential expiration date:** Date that the cardholder's credential expires.
- **Credential status:** The status of the cardholder or visitor's credential: Active; Inactive.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Description:** Description of the event, activity, entity, or incident.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 168 of 430

- **Email address:** Cardholder or visitor's email address.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **PIN:** Credential PIN.
- **Role:** Role type that manages the selected **Federated** or **Active Directory** imported entity.

3.8.19 Search for Credentials

If you have a large access control system and cannot find a credential, you can search for it by name, or use the advanced search by applying a combination of filters.

To Search for a Credential:

1. From the home page, open the **Credential management** task.
2. To search by an entity name, type the name in the **Search** (🔍) box. All entities with names that match the text you entered are listed.
3. To search for the entity using the advanced search:
 - A. In the left pane, click **Advanced search**.
 - B. Set up the query filters for the report. Choose from one or more of the following filters:
 - **Cardholders:** Restrict the search to certain cardholders.
 - **Credential:** Specify whether or not the credential is assigned.
 - **Credential information:** Restrict the search to specific **card formats**, **facility codes** or **card numbers**.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
 - **Description:** Restrict the search to entries that contain this text string.
 - **Expiration date:** Specify a time range for when the credential will expire.
 - **Partition:** Partition that the entity is a member of.
 - **Status:** The status of the cardholder or visitor's profile: **Active**; **Expired**; **Inactive**; **Lost**; **Stolen**. Not all statuses are available for every task.
 - **Unused credentials:** Search for credentials that have not produced an access granted event within a certain time range.
 - **NOTE:** For the report to generate results, all **Access Manager** roles must be active and online.
 - C. Click **Search**.

The credentials that match your search criteria are displayed on screen.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 169 of 430

3.8.20 Report Pane Columns for the Credential Management Task

After generating a report, the results of your query are listed in the **Report** pane. This section lists the columns available for the relevant reporting task.

- **Credential Activation date:** Date that the credential was activated.
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Cardholder activation date:** Date that the cardholder's profile was activated.
- **Cardholder expiration date:** Date that the cardholder's profile expires.
- **Cardholder status:** The cardholder's profile status.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **Credential expiration date:** Date that the cardholder's credential expires.
- **Credential status:** The status of the cardholder or visitor's credential: Active; Inactive.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Description:** Description of the event, activity, entity, or incident.
- **Email address:** Cardholder or visitor's email address.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.
- **PIN:** Credential PIN.
- **Role:** Role type that manages the selected entity.

3.9 AREAS AND DOORS

When you display an area () or a secured area () in a canvas tile, the area widget appears in the dashboard so you can control the area. Areas usually have multiple cameras attached to them. When you view an area, the first camera associated to that area is displayed.



Figure 114. View Area

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 170 of 430

By clicking the **eye** (👁️) icon in the **tile** toolbar, you can select which attached entity to view, or you can unpack the area, which displays all the attached entities in separate tiles. You can also start **entity cycling**, which rotates the entities displayed in the tile. If no camera is associated to the area, only the area icon is shown.

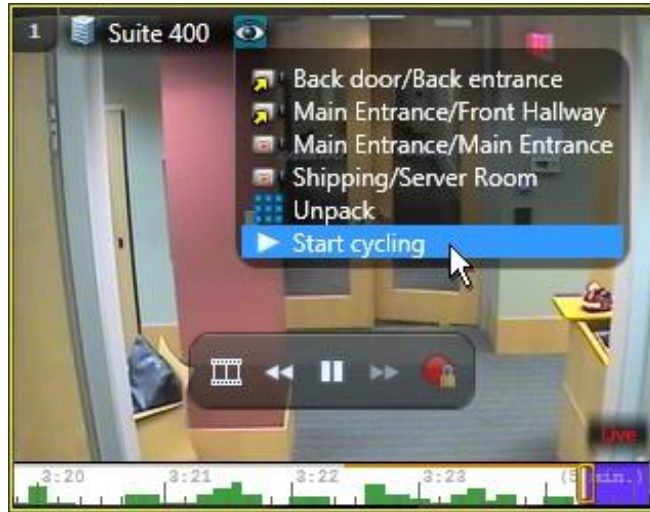


Figure 115. Entity Cycling

When you display a door (🚪) in a canvas tile, the door widget appears in the dashboard so you can control the door. If the door is linked to a camera, then the video stream of the camera is shown in the tile.



Figure 116. Video Stream in Tile

If the door is not linked to a camera, only the door icon is shown. The door image is static. It always remains open.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 171 of 430



Figure 117. Static Door Image

3.9.1 Allow Access through Doors

To unlock a door or override locking and unlocking schedules, you can use the Door widget to control access through doors. The door widget is enabled when a door entity is displayed in the selected canvas tile.

Access controlled doors are locked by default, unless an unlock schedule is being used. Only cardholders with the correct credentials can open them. When a door is displayed in a canvas tile, the door entity icon in the tile toolbar changes in real time to reflect whether the door is physically **open** (🚪) or **closed** (🔒).

If no camera is associated to the door, a static open-door image is displayed in the canvas tile. The following figure shows an open door and its corresponding door icon.

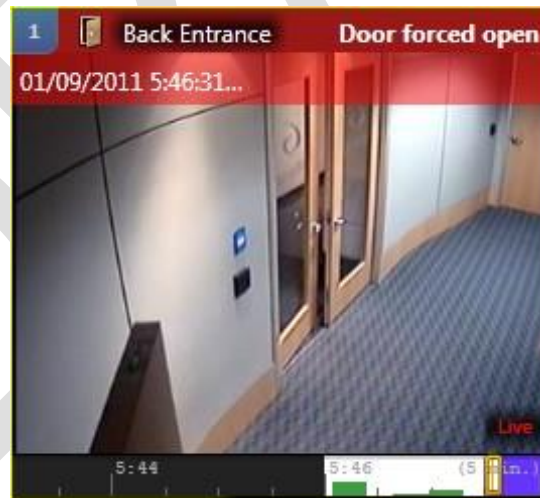


Figure 118. Door Entity

To Allow Access Through a Door:

1. From the **Monitoring** task, select a tile that is displaying a door.

The **Door** widget is displayed in the dashboard.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 172 of 430

2. In the **door** widget, do one of the following:

- To unlock the door and temporarily grant access, click **Unlock** (🔓).
- The duration of the grant time is configured by the system administrator. The widget shows that the door is open and unlocked.
- To override the door's unlock schedule, click **Override** unlock schedules (📅), and select one the following:
 - **Unlock for maintenance**: Unlock the door indefinitely for maintenance purposes. To cancel this override, click (🚫) in the **door** widget.
 - **Temporarily override unlock schedule**: Lock or unlock the door for the time specified in the From and To fields. With this option, the door returns to its normal state after the time expires.
 - **Example**: When setting unlock schedules for a door, a *Security Center* administrator can program a door to grant access to everyone during certain hours of the day, such as when a receptionist is on duty. If you have the rights, you can override these unlock schedules by locking the door when it is scheduled to be unlocked, or by unlocking the door when it is scheduled to be locked.

3.9.2 Prevent Access through Doors

To temporarily prevent all access through a door, you can deactivate (or shunt) the reader on the side of the door you don't want people to access.

Not all readers can be disabled from Security Desk. The ability to shunt a reader depends on your access control equipment. Shunting a reader is equivalent to cutting the power to the reader. For this reason, a cardholder presenting a valid credential at the door would no longer be able to unlock the door. This however does not prevent someone from unlocking the door with a key.

TIP: You can also shunt a defective reader to prevent it from beeping or generating any events.

To Prevent Access Through a Door:

1. From the **Monitoring** task, select a tile that is displaying a door. The **Door** widget is displayed in the dashboard.
2. In the **door widget**, click the **Reader** (📄) button, and select the reader you want to shunt. The reader that is shunted is indicated in the door widget.



Figure 119. Door Widget

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 173 of 430

3.9.3 Investigate Area Events

You can investigate events related to areas (Access granted, First person in, Antipassback violation, and so on), using the **Area activities** report.

To Investigate Area Events:

1. From the home page, open the **Area activities** task.
2. Set up the query filters for the report. Choose from one or more of the following filters:
 - **Areas:** Select the areas to investigate.
 - **Cardholders:** Restrict the search to certain cardholders.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
 - **Events:** Select the events of interest. The event types available depend on the task you are using.
 - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the previous week or the previous month.
3. Click **Generate report**. The area events are listed in the **Report** pane.
4. To show the corresponding video of an event in a tile, double-click or drag the item from the **Report** pane to the canvas. If the area is not associated to a URL or a map file through a tile plugin, the area icon is displayed.
5. To control the areas, use the area widget.
 - **Example:** If you want to see all the activity that went on in a particular area during the weekend, or since the last time you logged on, you can select a specific area and time range for the report. You can search for critical events that happened in an area (such as Access granted or Access denied: Stolen credential events), and then review the video associated with that event to see what happened during that time, and to find evidence.

3.9.4 Report Pane Columns for the Area Activities Task

After generating a report, the results of your query are listed in the **Report** pane. This section lists the columns available for the relevant reporting task.

- **Area:** Area name.
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Email address:** Cardholder or visitor's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 174 of 430

- **First name:** Cardholder or visitor's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Security clearance:** The cardholder's security clearance level.
- **Side-Direction:** Entrance or exit.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, or intrusion detection unit involved.

3.9.5 Investigate Door Events

You can investigate events related to doors (Door forced open, Door open too long, Hardware tamper, and so on), using the **Door activities** report.

To Investigate Door Events:

1. From the home page, open the **Door activities** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
 - **Cardholders:** Restrict the search to certain cardholders.
 - **Credentials:** Restrict the search to specific credentials.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
 - **Doors:** Select the doors to investigate.
 - **Events:** Select the events of interest. The event types available depend on the task you are using.
 - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the previous week or the previous month.
3. Click **Generate report**. The door events are listed in the **Report** pane.
4. To show the corresponding video of an event in a tile, double-click or drag the item from the **Report** pane to the canvas.

If there is no camera attached to the door, the door icon is displayed. To control the doors, use the **door** widget.

- **Example:** You can see how many access denied events have occurred in the last week, or since your last shift, or search for other critical events (For example, Door forced open). If you see suspicious cardholder activity while monitoring live video, you can investigate what other doors the cardholder accessed in the last day. If you want to see if the maintenance staff has completed work at a particular door, you can investigate on that door, and select the Door maintenance completed event.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 175 of 430

3.9.6 Report Pane Columns for the Door Activities Task

After generating a report, the results of your query are listed in the **Report** pane. This section lists the columns available for the relevant reporting task.

- **NOTE:** If you generated the Door activities report using Web Client, not all of the report columns are available.
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Door:** Door name.
- **Email address:** Cardholder or visitor's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder or visitor's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Side:** Door side name.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, or intrusion detection unit involved.

3.9.7 Identify Who is Granted/Denied Access at Access Points

You can find out which cardholders are currently granted or denied access to selected areas and doors, using the **Cardholder access rights** report. This report is helpful because it allows you to see where a cardholder can go, and when, and determine if their access rule properties must be adjusted.

- **TIP:** Perform your query on one access point at a time, so your report is more specific.

To Identify Who is Granted/Denied Access at an Access Point:

1. From the home page, open the **Cardholder access rights** task.
2. Set up query filters for your report. Choose one or more of the following filters:
 - **Doors - Areas:** Restrict the search to activities that took place at certain doors and areas.
3. Click **Generate** report.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 176 of 430

The cardholders associated with the selected access point through an access rule are listed in the **Report** pane. The results indicate if the cardholder is granted or denied access, and by which access rule.

4. To show a cardholder in a tile, double-click or drag a cardholder from the **Report** pane to the canvas.
5. To view additional cardholder information in the tile, click (i).
6. After you finish, if necessary, modify the cardholder's access rights.

3.9.8 Report Pane Columns for the Cardholder Access Rights Task

After generating a report, the results of your query are listed in the **Report** pane. This section lists the columns available for the relevant reporting task.

- **Cardholder:** Cardholder entity name.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Denied access by:** Access rules denying access to at least one of the selected entities to the cardholder.
- **First name:** Cardholder or visitor's first name.
- **Granted access by:** Access rules granting the cardholder access to at least one of the selected entities (area, door, etc.).
- **Last name:** Cardholder or visitor's last name.
- **Member of:** All groups the cardholder belongs to.
- **Picture:** Cardholder or visitor's picture.

3.9.9 Identify Who is Granted Access to Doors

You can verify which cardholders are granted access to a particular door side at a specific date and time, using the **Door troubleshooter** report. This report is helpful, because it allows you to see what the configuration of a door is and determine if their properties must be adjusted. The door troubleshooter does not examine each cardholder's credentials. You can further diagnose the cardholder's access rights using the Access troubleshooter tool.

To Identify Who is Granted Access to a Door:

1. From the home page, open the **Door troubleshooter** task.
2. In the **Filters** tab, select a date and time for the report.
3. Select a door you want to investigate.
4. From the **Access point** drop-down list, select the access point (door side) you want to verify.
5. Click **Generate report**. All cardholders who can go through the selected access point at the specified time are listed in the **Report** pane.
6. After you finish, if necessary, test your access control configuration.

3.9.10 Report Pane Columns for the Door Troubleshooter Task

After generating a report, the results of your query are listed in the **Report** pane. This section lists the columns available for the relevant reporting task.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 177 of 430

- **Cardholder:** Cardholder entity name.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **First name:** Cardholder or visitor's first name.
- **Last name:** Cardholder or visitor's last name.
- **Picture:** Cardholder or visitor's picture.

3.9.11 Identify Entities Affected by Access Rules

You can find out which entities and access points are affected by a given access rule, using the **Access rule configuration** report.

In the report results, you can see the members of the access rule, such as the cardholders, doors, and the associated schedule. This helps you determine if you must add or remove entities or adjust the schedule.

To Identify Which Entities are Affected by an Access Rule:

1. Open the **Access rule configuration** task.
2. Set up the query filters for your report. Choose one or more of the following:
 - **Access rule:** Select the access rule to investigate.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
3. In the **Expand cardholder groups** option, select **Enable** to list the members of the affected cardholder groups in the report instead of the cardholder groups themselves.
4. In the **Include perimeter entities** option, select **Enable** to include the perimeter entities of the affected areas in the report.
5. Click **Generate report**.

The entities and access points affected by this access rule are listed in the **Report** pane.

3.9.12 Report Pane Columns for the Access Rule Configuration Task

After generating a report, the results of your query are listed in the **Report** pane. This section lists the columns available for the relevant reporting task.

- **Access point:** Access point involved (only applicable to areas and doors).
- **Access rules:** Name of the access rules.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Icon:** Graphical representation of the affected entity type.
- **Member:** Name of the affected entity.
- **Type:** Affected entity type.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 178 of 430

3.10 USER MANAGEMENT

The **User management** task is a type of **administration** task that allows you to configure users, user groups, and partitions.

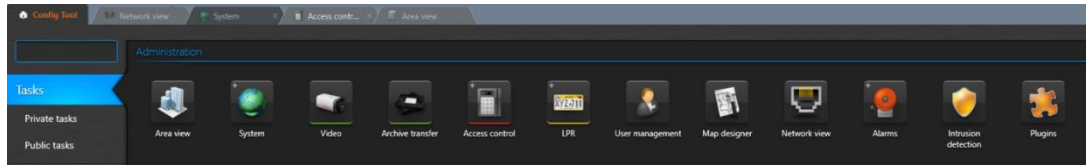


Figure 120. User Management: Config Tool

Security Center manages (internal) security through three entities: Users, User Groups and Partitions.

- For **Users** and **User Groups**, the assigned privileges define what the user can do.
- For **Partitions** (which HART does not use) access rights define which entities users can see or access

3.10.1 User Properties

User properties include options such as

- Password expiration
- User priority level
- Access rights
- Privileges
- Logon hours
- Default tasks
- Remote control

3.10.2 User Privileges

User privileges define what applications can be used, which tasks a user can open, and what you can within those tasks.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 179 of 430

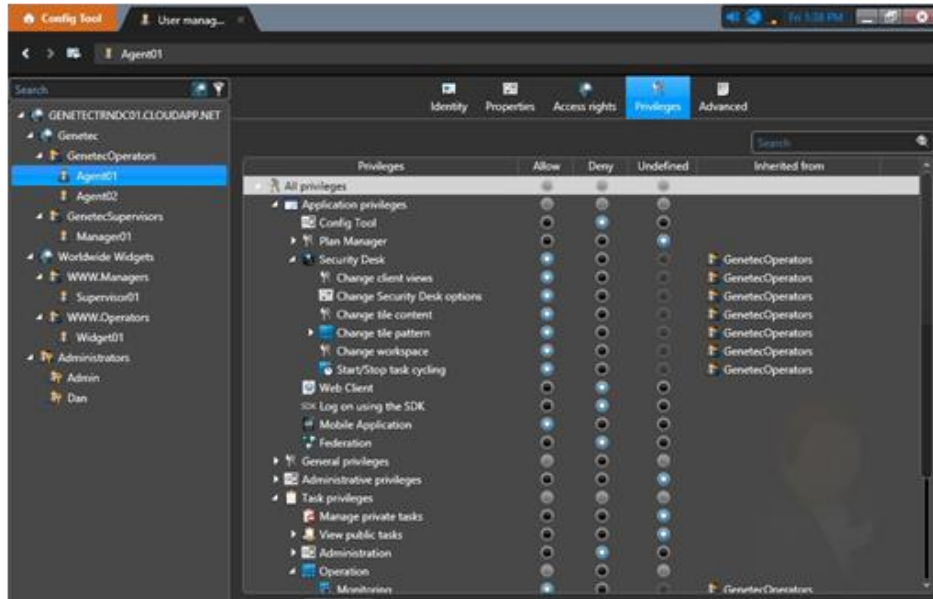


Figure 121. User Management: User Privileges

3.10.3 Unconfigured Users

An unconfigured user is a newly created user has no privileges by default. If the user wasn't created using a privileges template and that user does not belong to any user group, all privileges are undefined.

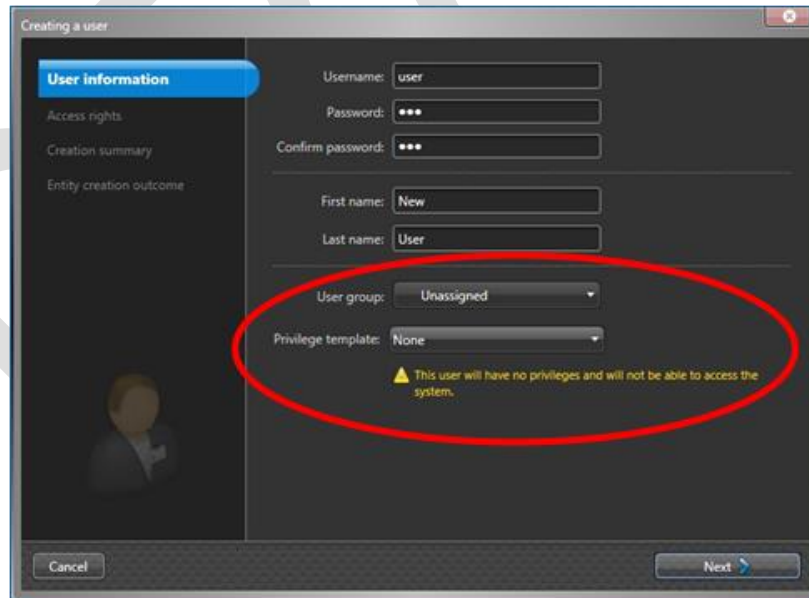


Figure 122. User Management: Unconfigured User

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 180 of 430	

3.10.4 Remote Control

Remote control is a type of operation task that allows you to remotely monitor and control other Security Desks that are part of your system using the **Monitoring task** and the **Alarm monitoring task**.

To gain remote control access of another user's monitor

1. Go to **Security Desk** tab and select the **Monitoring task**.
2. To open a new task, right-click the **Home tab** and select **New Task** from the dropdown menu.
3. Drag and drop a tile from a location on the left pane to the **Area View**.
 - To change the tile pattern on a remote workstation, click the **Change Tile Patterns** button at the bottom of the screen.
 - To disconnect from a remote workstation, click the **Disconnect** button at the top right corner

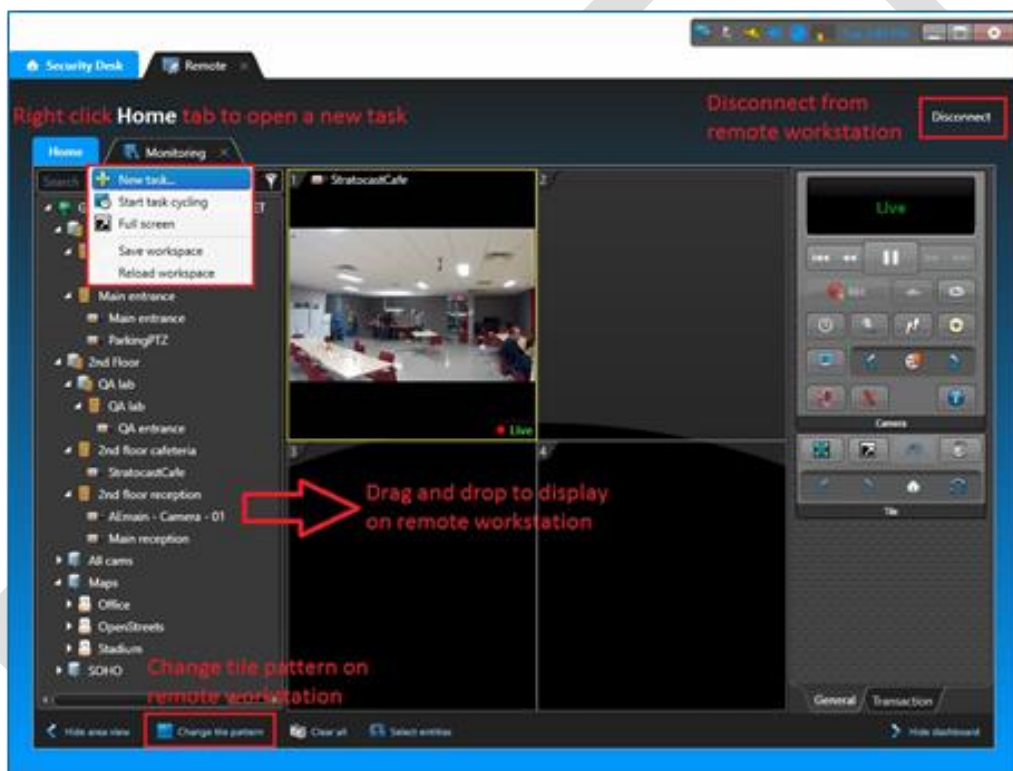


Figure 123. User Management: Remote Control

3.10.5 User Groups

A user group's members can be users, or other user groups. Group privileges are inherited by group members. All user configurations are available at the group level except:

- Password settings.
- Security Desk default tasks.
- Logon schedules.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 181 of 430

3.10.6 Resolve Conflicting Privileges

Users can belong to multiple groups, and groups can contain subgroups, but sometimes privileges may conflict. So, which takes priority, the user privilege or the group privilege? Answer: Neither. 'Deny' overrides 'Allow' and 'Allow' overrides 'Undefined'.



Figure 124. User Management: Resolving Conflicting Privileges

3.10.7 Users

A user is a type of entity that identifies a person who uses *Security Center* applications and defines the rights and privileges that person has on the system. Users can be created manually or imported from an **Active Directory**. Each user is assigned a username and a password, which are the credentials required to log on to the system.

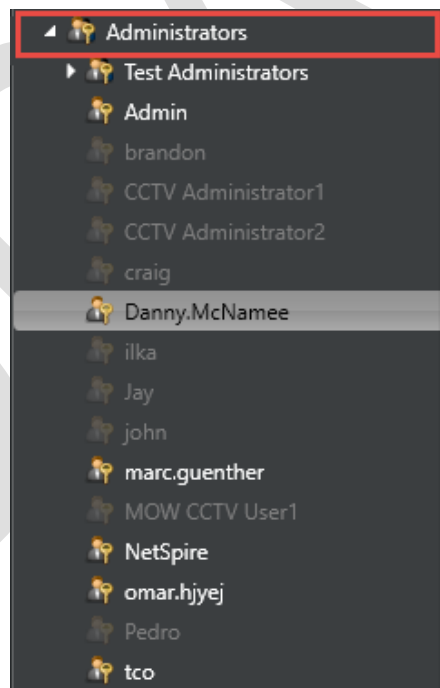


Figure 125. User Management: Users

What a person can do on the system is restricted by their user attributes:

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 182 of 430

- **Privileges:** Limits the types of activities the user can perform on the system.
- **Access rights for partitions:** Limits the entities the user can exercise their privileges on.

A user can be a member of one or more user groups. Users can inherit the privileges and the access rights from their parent user groups.

Admin user

The Admin user is a user created by default and cannot be deleted or renamed. It has full administrative rights to configure *Security Center*. A person logged on as Admin can add, modify, and delete any entity in *Security Center*.

- **BEST PRACTICE:** The Admin user is created with a blank password at software installation. For security reasons, you should immediately change the Admin user's password after software installation.

User levels

A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera PTZ, viewing the video feed from a camera, or staying logged on when a threat level is set. Level 1 is the highest user level, with the most privileges. User levels range from 1-254. The user level can be inherited from a parent user group. If the user has multiple parents, the highest user level is inherited. If the user has no parent group, the lowest user level (254) is inherited.

User levels affects four things in *Security Center*.

- They determine which users are logged out of the system when a threat level is set. For example, if you configure a threat level to trigger the Set minimum user level action, when the threat level is set, users with a lower user level than the one you specified are logged off.
- They determine which users can continue viewing a video stream when a camera is blocked in Security Desk. When you block a camera, users that have a lower user level than the one you specified can no longer view the video stream.
- They determine which users lose their video stream connections if a maximum bandwidth limit is configured for video streams that are redirected from a remote site, and the bandwidth limit is exceeded. When the bandwidth limit is reached and a user with a high user level requests a stream, the user with the lowest user level who is currently viewing video that is being redirected through that redirector loses their stream connection. If multiple users with the same user level are viewing video streams from that redirector, the user who requested the video stream last loses the stream connection.
- They determine which user has priority over the **PTZ** controls of a camera when two or more users are trying to take control of a camera at the same time.
- Users can be given different user levels for **PTZ** controls that override their general user level. Priority is always given to the user with the highest level (1=highest). If two competing users have the same user level, the user who requested the stream first is given priority.

3.10.7.1 Create a User

To allow someone to log on to *Security Center*, you must create a user entity for them with logon credentials. You can also import users from your corporate directory service.

For security purposes, the Entity name for this user must be unique, because it is also the username they use to log on to *Security Center*.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 183 of 430

To Create a User:

1. From the **Config Tool** home page, open the **User management** task.
2. Click **Add an entity**, then click **User**.
3. In the **User information** page, enter a username that does not already exist.
4. Type a password for this user to log on to *Security Center*, and then confirm the password.
5. Enter the user's first and last name.
6. From the **User group** drop-down list, select the parent group for the new user. The user automatically inherits the properties of its parent user group.
 - **NOTE:** Concerning the user's partition membership:
 - If you select **Unassigned**, the new user will be added to the root partition.
 - If you select a parent user group, the new user will be added to the same partition that the parent user group belongs to.
7. To grant the user a predefined set of privileges, select a **Privilege** template from the drop-down list.
 - **NOTE:** If you are unsure of what privileges the user needs, you can postpone this decision to later. The privilege template can be applied at any time.
8. Click **Next**.
9. In the **Creation summary** page, verify that both the partition the user belongs to and the ones the user is authorized to access are as you intended.
10. Click **Create > Close**. The new user account is created.
11. After you finish, configure the user.

3.10.7.2 Configure User Settings

After a user is created in *Security Center*, you can configure their properties, and limit what they are allowed to do on the system.

Before you begin, create the user. Instead of configuring the properties of an individual user, you can add the user as a member of a user group, so they inherit all the properties of the group.

To Configure a User's Settings:

1. From the **Config Tool** home page, open the User management task.
2. Select the user to configure, and click the **Properties** tab.
3. To temporarily prevent the user from logging on to *Security Center*, deactivate the user profile.
4. If you want to send emails or messages to this user, type an email address in the **Email address** field, and click **Apply**.
5. You can send emails to users using the **Send an email** and **Email a report actions**.
6. Change the user's password or their password settings.
7. In the **User level** option, specify if the user inherits their user level from its parent user group, or set a specific level, and click **Apply**.
 - A user level is a numeric value assigned to users to restrict their ability to perform certain operations, such as controlling a camera **PTZ**, viewing the video feed from a camera, or staying logged on when a threat level is set. **Level 1** is the highest user level, with the most privileges.
6. Optional: Configure a different user level for controlling **PTZ** motors.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 184 of 430

8. Grant access rights for partitions to the user.
9. Assign privileges to the user.
10. Customize how the user can log on.
11. To allow the user to remotely control *Security Desk* workstations, you must select the workstations they can control.
12. Click the **Advanced** tab.
13. To cycle the user's open tasks when they log on to *Security Desk*, switch the **Start task cycling** on logon option to **ON**, and click **Apply**.
 - **TIP:** To prevent the user from stopping the task cycling once the *Security Desk* is open, deny them the **Start/stop task cycling** privilege.
14. When the user exports video (G64x) or snapshots, the system can include metadata (for example, camera name, creation date, and camera coordinates) which can be useful in incident investigation. To enable metadata with exported files, switch the **Include additional properties on export/snapshot** option to **ON** and click **Apply**.

Deactivate a User Profile

You can deactivate the profile of users that should no longer be allowed to log on to *Security Center*. A user cannot log on when their profile is deactivated. Deactivating a user's profile while the user is logged on will immediately log off the user.

To Deactivate a User's Profile:

1. From the **Config Tool** home page, open the **User management** task.
2. Select the user to configure, and click the **Properties** tab.
3. Switch the **Status** option to **Inactive** and click **Apply**.

3.10.7.3 Change Password Settings for Users

You can set a user's password to expire after a certain amount of time, force users to change their password on next logon, or enforce a minimum complexity for all user passwords. Password complexity requirements apply to all new passwords and take effect when a user changes their current password.

Only users who have the **Change own password** user privilege can change their own password. Otherwise, they must contact their administrator to change their password.

To Change the Password Settings for a User:

1. From the **Config Tool** home page, open the **User management** task.
2. Select the user to configure, and click the **Properties** tab.
3. To change the user's password, click **Change password**, type a password, confirm the password, and click **OK**.
4. To set an expiry date for the user's password, switch the **Expires** option to **ON**, and select the number of days.
 - The system automatically warns users if their passwords are expiring soon and gives them a chance to set a new password immediately. You can set the password expiry notification period to between 0 and 30 days from the **System** task.
5. To require the user to change their password the next time they log on to Genetec Patroller™ or *Security Desk*, switch the **Change on next logon** option to **ON**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 185 of 430

6. Click **Apply**.
7. To add complexity requirements to user passwords, open the System task, click the **General settings** view, and click the **User password settings** page.
8. In the **Enforce a minimum number of** section, select from the following requirements, and type a value:
 - **Characters:** Minimum number of characters.
 - **Upper case letters:** Minimum number of upper-case letters.
 - **Lower case letters:** Minimum number of lower-case letters.
 - **Numerical characters:** Minimum amount of numbers.
 - **Special characters:** Minimum number of special characters.
9. Click **Apply**.

3.10.7.4 Customize User Logon Options

You can select how and when users are allowed to log on to *Security Center*. The settings apply to the local workstation and affect Security Desk and **Config Tool** for all users. Changes only take effect the next time a user starts Security Desk or **Config Tool**.

- **NOTE:** If Use **Windows** credentials is set to **Always** or the **Force Directory** to option is selected, and a user is stuck and cannot log on, hold **Ctrl+Shift**, and click **Log on**. This either lets the user log on using their *Security Center* credentials or forces the **Directory** field to be displayed.

To Customize User Logon Options:

1. From the home page in **Config Tool**, click **Options > General**.
2. To force users to log on using **Windows** credentials, set the **Use Windows credentials** option to **Always**.
 - For this option to work, the users who are expected to log on using this computer must be imported from an **Active Directory**.
3. To restrict the access of all users to a specific **Directory**, select the **Force Directory** to option, and type the name of the **Directory**.
 - With this option, users cannot choose the Directory to which they want to connect; the **Directory** field is not displayed in the **Logon** window. However, they can automatically be redirected to another **Directory** when load balancing is used.
 - **NOTE:** If there is a mistake in the **Directory** name (for example, a typo), then the next time users try to log on, they will not be able to connect.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 186 of 430

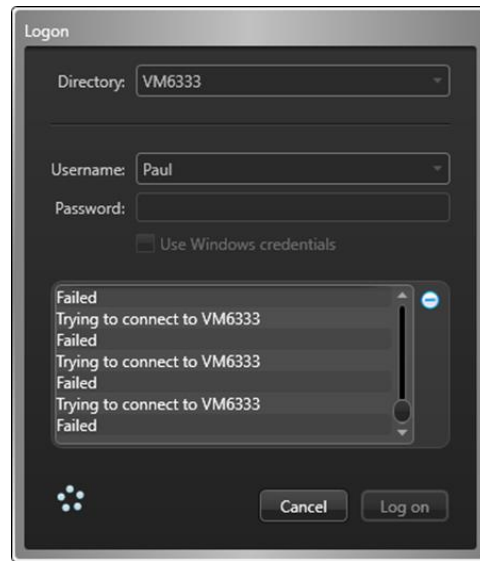


Figure 126. Logon

4. To bypass **Directory load balancing**, select the **Prevent connection redirection** to different Directory servers option.

Users will connect to the default Directory or to the Directory they specify when logging on and will not be automatically redirected to another server. This option is meaningful only if Directory load balancing is configured.
5. Click **Save**.
6. To limit the number of workstations a user can log on to at the same time, do the following:
 - A. Open the **User management** task.
 - B. Select the user you want to configure, and click the **Advanced** tab.
 - C. Switch the **Limit concurrent logons** option to **ON** and select the number of workstations.
7. To select when a user can log on, click **Add an item** (+) under the **User logon schedule** section.
8. Select predefined schedules and click **Select**.
9. If you select multiple schedules, the schedule conflict rules apply. When two schedules with the same priority level overlap, the blocking schedule has priority over the allowing schedule.
10. To lock the user's session after a period of inactivity, switch the **Auto lock** option to **ON**, and select how long the session must remain inactive before being locked.
11. This option only applies to Security Desk. Before being locked, the message **Session** is about to lock is displayed to the user. After the application is locked, the user must log back on to resume with the current session.
 - **NOTE:** If the user is authenticated through ADFS with passive authentication, the user will be logged off and their current session closed instead of being locked.
12. Click **Apply**.
13. To require the user to log on to *Security Center* with a logon supervisor, in the **User management** task, select the user to be the supervisor, and click the **Advanced** tab.
14. Under the **Logon supervisor of section**, click **Add an item** (+), select the user to be supervised,

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 187 of 430

and click **OK**.

15. Click **Apply**.

3.10.7.5 Access Rights

An access right is the basic right users must have over any part of the system before they can do anything with it. Other rights, such as viewing and modifying entity configurations, are granted through privileges. In the context of a Synergis™ system, an access right is the right granted to a cardholder to pass through an access point at a given date and time.

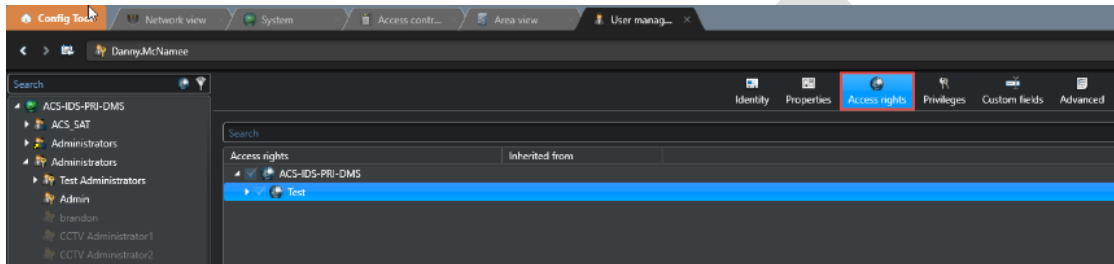


Figure 127. User Management: Access Rights

3.10.8 User Groups

A user group is a type of entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the properties of the group. A user can be a member of multiple user groups. User groups can also be nested.

A user group is a type of entity that defines a group of users who share common properties and privileges. By becoming member of a group, a user automatically inherits all the properties of the group. A user can be a member of multiple user groups. User groups can also be nested.

Benefits of user groups

Since all the users that are part of the user group automatically inherit all the properties of that group, this simplifies the configuration of users on large systems.

Administrator's user group

The Administrators user group is a system entity that is created during installation. It cannot be deleted or renamed. Members of this user group are also known as system administrators. They have the same administrative rights as the Admin user, and their rights cannot be revoked.

- **BEST PRACTICE:** For reasons of traceability, rather than letting everyone use the same Admin account, it is best to create a separate user account for each administrator.

3.10.8.1 Create A User Group

To group users who share common properties and privileges, you can create user groups. You can also import user groups from your corporate directory service.

To Create a User Group:

1. From the **Config Tool** home page, open the **User management** task.
2. Click **Add an entity** (+), then click **User group** (person icon).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 188 of 430

3. In the **User group information** page, enter a name and description for the user group.
4. From the **User group** drop-down list, select the parent group for the new user group. The user group automatically inherits the properties of its parent user group.
 - **NOTE:** Concerning the user group's partition membership:
5. If you select **Unassigned**, the new user group will be added to the root partition.
6. If you select a parent user group, the new user group will be added to the same partition that the parent user group belongs to.
7. To grant the user group a predefined set of privileges, select a **Privilege** template from the drop-down list.
 - **NOTE:** If you are unsure of what privileges the user group needs, you can postpone this decision to later. The privilege template can be applied at any time.
8. Click **Next**.
9. In the **Creation summary** page, verify that both the partition the user group belongs to and the ones the user group is authorized to access are as you intended.
10. Click **Create > Close**. The new user group is created.
11. Optional: Make this user group a subordinate of another user group.

Add Subordinate User Groups

To save time on configuring your system, you can create sub-user groups that inherit all the attributes of their parent group.

Adding sub-user groups is helpful if you have multiple levels in your management team, and the sub-groups share almost all the same properties and privileges (for example, a day shift user group and a night shift user group on your security team).

To Add a Subordinate User Groups

1. Open the **Security** task and click the **User groups view**.
2. Select the user group to configure.
3. In the **Relationships** section of the **Identity** tab, select **Parent user groups**, and click **Insert an item** (In the Relationships section of the Identity tab, select Parent user groups, and click Insert an item (+)).
4. Select one or more parent user groups and click **Select > Apply**.
 - **TIP:** Alternatively, you can modify the user groups' membership directly from the entity tree, using **drag-and-drop** to move, and **Ctrl+drag-and-drop** to copy.

3.10.8.2 Force Security Desk to Run in Full Screen Mode

If a user's job is to focus on monitoring live video, you can force Security Desk to run in full screen mode to prevent the user from switching to **Windows** mode. You can also set Security Desk to start in full screen operation mode on a specific workstation.

To Force Security Desk to Run in Full Screen Mode for a User:

1. From the **Config Tool** home page, open the **User management** task.
2. Select a user, and click the **Privileges** tab.
3. Expand the **Application** privileges, and the **Security Desk** privileges.
4. Deny the privilege **Change client views** to that user.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 189 of 430

5. Click **Apply**.

Security Desk now always runs in full screen mode for that user. The **Restore Down** command and the **F11** key (switch between full screen and windowed mode) are disabled.

Setting Security Desk to Start in Full Screen Mode on Workstations

If a workstation is mainly used for monitoring live video, you can set Security Desk to always start in full screen mode on that workstation. Setting Security Desk to start in full screen mode does not prevent the user from minimizing the Security Desk window with **Alt+ESC** or to switch to another application with **Alt+Tab**.

To Set Security Desk to Start in Full Screen Mode on a Workstation:

1. On the workstation, open the Security Desk **Properties** dialog box.
2. Select the **Shortcut** tab and add the option `/forcefullscreen` (or `/ff`) to the end of the string found in Target.
3. Click **Apply**.

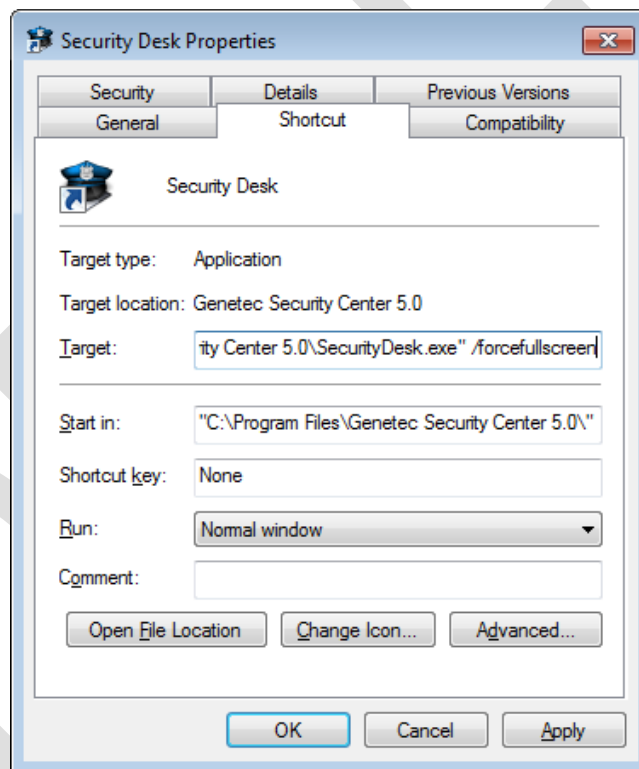


Figure 128. Security Desk Properties

The next time a user starts Security Desk using this shortcut, the application starts in full screen mode. The **Restore Down** commands and the **F11** key (switch between full screen and windowed mode) are disabled.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 190 of 430

3.10.8.3 Select Which Workstations Users Can Remotely Control

You can select which Security Desk workstations and monitors a user is allowed to remotely control using a CCTV keyboard or using the **Remote** task in *Security Desk*.

Every monitor controlled by *Security Desk* is assigned a unique monitor ID (displayed in the notification tray and found in the **General settings - Logical ID** page in the **System** task). Using a CCTV keyboard, you can display an entity on a remote Security Desk workstation by specifying its **monitor ID**, **tile ID**, and the **logical ID** of the entity.

- **IMPORTANT:** In addition to having the remote control rights over Security Desk workstations and users, the following conditions must also be met for a local user to be able to connect to a remote Security Desk workstation:
 - Both local and remote *Security Desk* must be running and connected to the same *Security Center* Directory.
 - The local user must have the same or more user privileges than the remote Security Desk user. The local user must have the same access rights, to all the partitions, as the remote Security Desk user.

To Select Which Workstations a User Can Remotely Control:

1. From the **Config Tool** home page, open the **User management** task.
2. Select the user to configure, and click the **Advanced** tab.
3. Under the **Allow remote control over** section, click **Add an item** (+).
4. From the drop-down list, select one of the following entity types:
5. **User:** Any *Security Desk* workstation where that user is logged on can be remotely controlled.
6. **User group:** Any *Security Desk* workstation where a member of that user group is logged on can be remotely controlled.
7. **Application:** The specified workstation (COMPUTER – *Security Desk*) can be remotely controlled, regardless of who is logged on.
8. Select the associated entities and click **OK > Apply**.

3.10.8.4 Select Which User Activities to Log

You can select which types of user-related activity are logged in the database, and available for reporting in the **Activity trails** task.

The activities you can log are events that are generated by users who connected to Security Center.

To Select Which User Activities to Monitor:

1. From the **Config Tool** home page, open the **System** task.
2. Click the **General settings** view, and then click the **Activity trails** page.
3. From the list, select the events to monitor. You can select general events, or events specifically related to video or access control.
4. Click **Apply**.

You can now search for events in your system that were triggered by users, using the **Activity trails** task.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 191 of 430

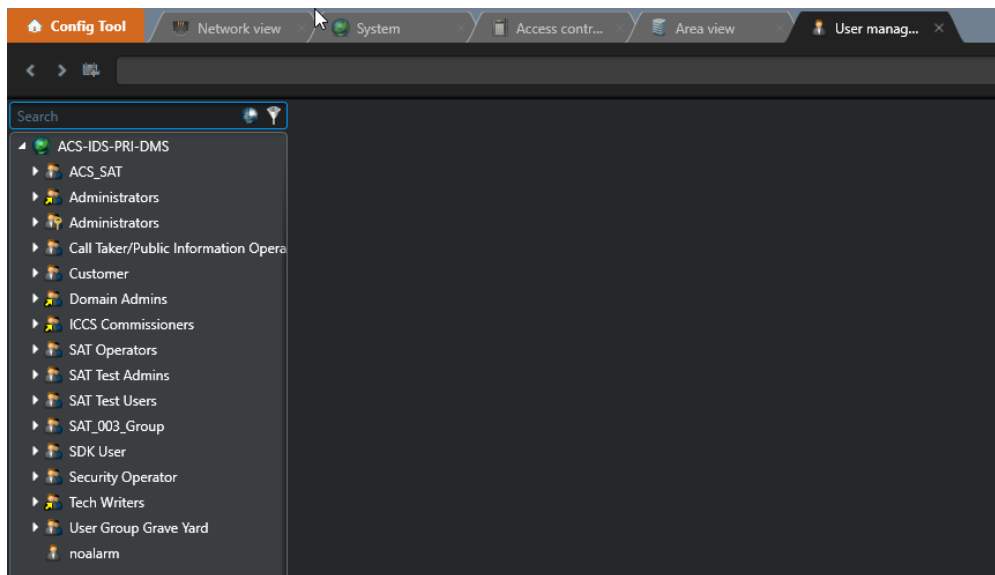


Figure 129. User Management: Config Tool - User Groups

3.10.9 Privileges

Privileges define what users can do, such as arming zones, blocking cameras, and unlocking doors, over the part of the system they have access rights to.

User privileges in *Security Center* are divided into the following groups:

- **Application privileges:** Grant access to the *Security Center* applications.
- **General privileges:** Grant access to the generic *Security Center* features.
- **Administrative privileges:** Grant access to entity configuration in **Config Tool**.
- **Task privileges:** Control accessibility to the various *Security Center* tasks.
- **Action privileges:** Control the actions that can be performed on the system entities.

For a list of available privileges, see **Security Center 5.7 Privileges on the Genetec™ TechDoc Hub**. You can also refer to the **Privileges** page of a user or user group in the **Config Tool User management** task.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 192 of 430

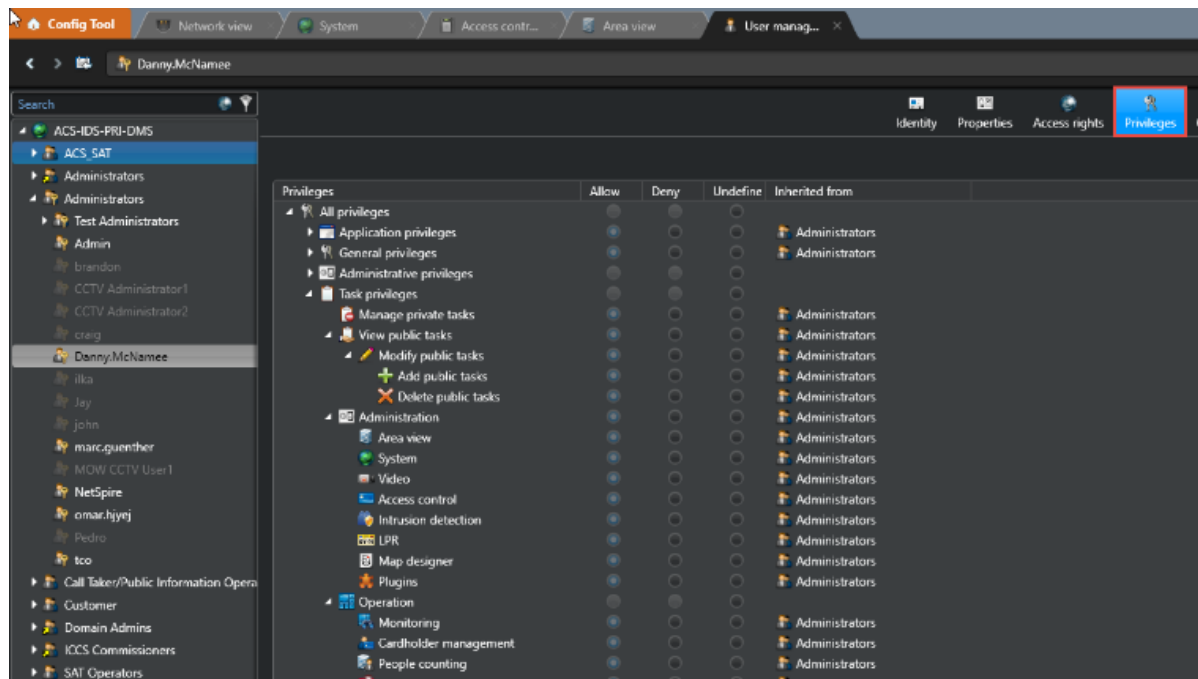


Figure 130. User Management: Privileges

Privilege hierarchy

Privileges are organized in a hierarchy, with the following behavior:

- For a child privilege to be allowed, the parent privilege must be allowed.
- If a parent privilege is denied, all child privileges are denied.
- A child privilege can be denied when the parent privilege is allowed.

Privilege inheritance

Privilege settings can be inherited from user groups and replaced at the member (user or user group) level according to the following rules:

- A privilege that is undefined at the group level can be allowed or denied at the member level.
- A privilege that is allowed at the group level can be denied at the member level.
- A privilege that is denied at the group level is automatically denied at the member level.
- When a user is a member of multiple user groups, the user inherits the most restrictive privilege settings from its parents. This means that Deny overrules Allow and Allow overrules Undefined.

Exceptions to privilege rules

The following exceptions apply to the privilege rules:

- **Administrative users:** Members of the Administrators user group (which include the Admin user) have full administrative rights over the system. They can configure *Security Center* as they see fit. The Admin user and the Administrators user group are created at system installation. They have all the privileges and cannot be modified nor deleted.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 193 of 430

- **Actions reserved for administrative users:** There are actions that only administrative users can perform because they can potentially affect the entire system. These actions are not associated to any privilege.
 - Adding, modifying, and deleting macros.
 - Viewing, adding, modifying, and deleting threat levels.
 - Creating generic event-to-actions (without a specific source entity).
 - Configuring archive transfers (using the Archive transfer task).
 - Configuring the general settings from the Access control task (card request reasons, custom card format, and so on).
 - Running the Import tool.
 - Running the Diagnostic data collection tool.

3.10.9.1 Privilege Templates

Privilege templates are predefined privilege configurations, based on standard security personnel profiles, that you can apply to users and user groups to simplify the creation process. Once applied, you can fine tune the privileges manually.

You cannot rename, modify, create, or delete privilege templates, but you can apply them at any time. You can freely modify the privilege settings after a privilege template is applied to a user or user group.

BEST PRACTICE: Create one user group for each privilege template if necessary. After your model user groups are created, users can inherit privileges from them.

Types of privilege templates

Security Center provides the following privilege templates:

Reporting: This template only grants the privileges to run Security Desk and to execute the most basic reporting tasks, excluding those for AutoVu™ LPR. A user with this set of privileges alone cannot view any video, control any physical devices, or report incidents.

Operator: This template is for security operators who need to monitor real time events in the system. It grants them the privileges to use the Monitoring task, view video, manage visitors, credentials, and badge templates, add bookmarks and incidents, save snapshots, unlock doors, and so on.

Investigator: This template is for investigators. It grants the privileges to use the Monitoring task, view video, control PTZ cameras, record and export video, add bookmarks and incidents, use investigation tasks, manage alarms and visitors, override door unlock schedules, save tasks, and so on.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 194 of 430

Supervisor: This template is for people who have supervisory responsibilities. It grants the same privileges as the Investigator template, plus the privileges to use maintenance tasks, manage cardholders and credentials, modify custom fields, set threat levels, block cameras, and perform people counting.

Provisioning: This template is for the system installer. It grants almost all configuration privileges, with only a few exceptions (managing roles, macros, users, user groups, custom events, activity trails, threat levels, and audio files).

3.10.9.2 Assign Privileges to Users

You must grant privileges to users in order for them to do anything in *Security Center*, including logging on, using Security Desk, and so on.

Users have a set of basic privileges, which are privileges explicitly granted to them or inherited from their parent user groups, plus a set of privileges for every partition for which they are an authorized user.

Privileges granted or denied at the partition level replace the basic privileges.

You can grant specific privileges to individual users or allow users to inherit privileges from their parent user groups.

To assign privileges to a user:

7. To set Security Desk to start in full screen mode on a workstation From the **Config Tool** home page, open the **User management** task.
8. Select the user to configure, and click the **Privileges** tab.
9. Use one of the predefined privilege configurations as your starting point. At the bottom of the page, click (⚙️), and select one of the following:
 - **Apply template:** Select one of the privilege templates to apply.
 - **Privilege templates can be combined.** This means that when you apply a privilege template, you always add privileges. Existing privileges can never be removed as a result of applying a privilege template. To start with a clean slate, go to the top of the privilege hierarchy (All privileges) and click **Undefined**.
 - **Set configuration to read-only:** Set all entity configuration privileges found under the **Administrative** privileges group to **View** properties with **Modify** properties denied.
Set configuration to read-write: Set all entity configuration privileges found under the **Administrative** privileges group to **View, Modify, Add, and Delete**.
10. Fine tune the user privileges by changing the individual privilege settings if necessary.
11. Keep in mind that if your user has a parent user group, the privilege inheritance rules apply.
 - **Allow:** Grant the privilege to the user. You cannot select this option if the privilege is denied to the parent user group.
 - **Deny:** Deny the privilege to the user.
 - **Undefined:** Inherit this privilege from the parent user group. If there is not parent user group, this privilege is denied.

If necessary, configure the privilege exceptions for each partition the user has access to. When a

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 195 of 430

user is given access to a partition, their basic privileges are applied by default to the partition. As a system administrator, you can overwrite the privileges a user has over a specific partition. For example, a user can be allowed to configure alarms in partition A, but not in partition B. This means that a user can have a different set of privileges for each partition they have access to. Only Administrative and Action privileges, plus the privileges over public tasks, can be overwritten at the partition level.

- A. At the bottom of the page, click **Exceptions (+)**. The **Privilege** exception dialog box opens.
- B. In the **Create an exception for** drop-down list, select a partition.
- C. Change the user's basic privileges as required.

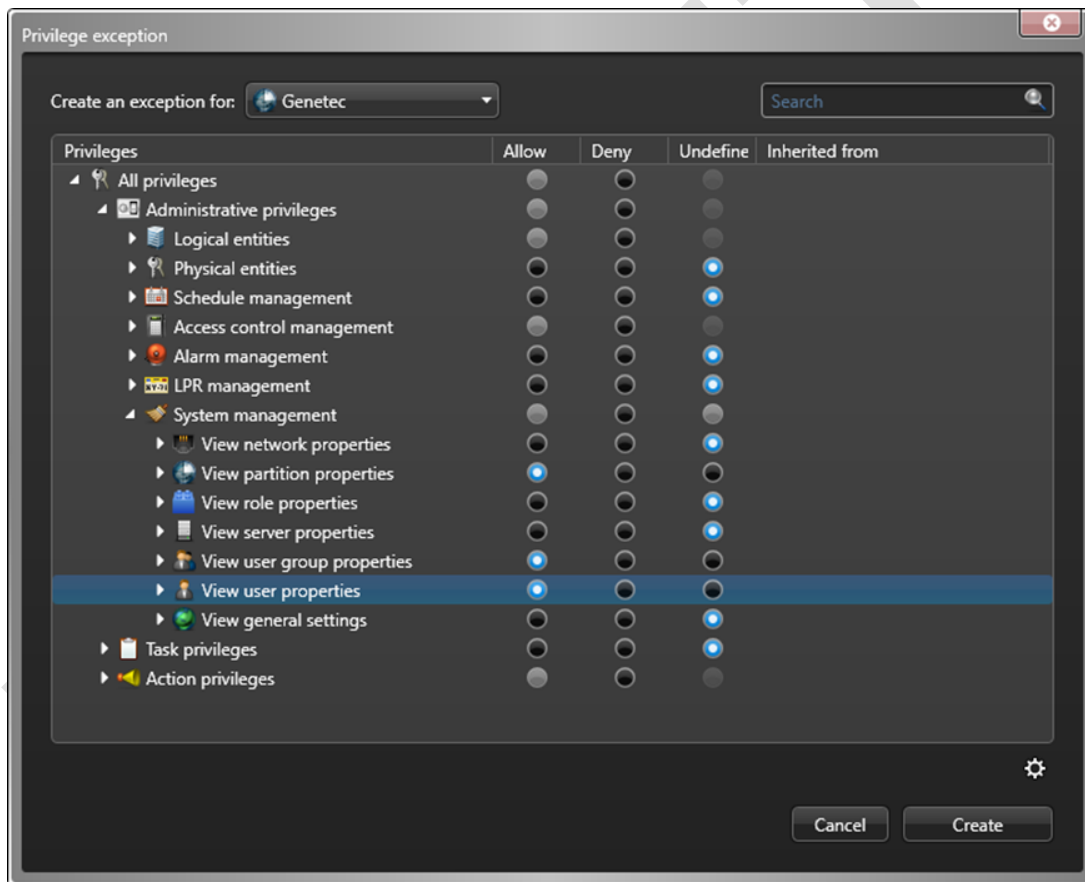


Figure 131. Privilege Exception

- D. Click **Create**.

The privilege exceptions are added at the bottom of the privilege list.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 196 of 430

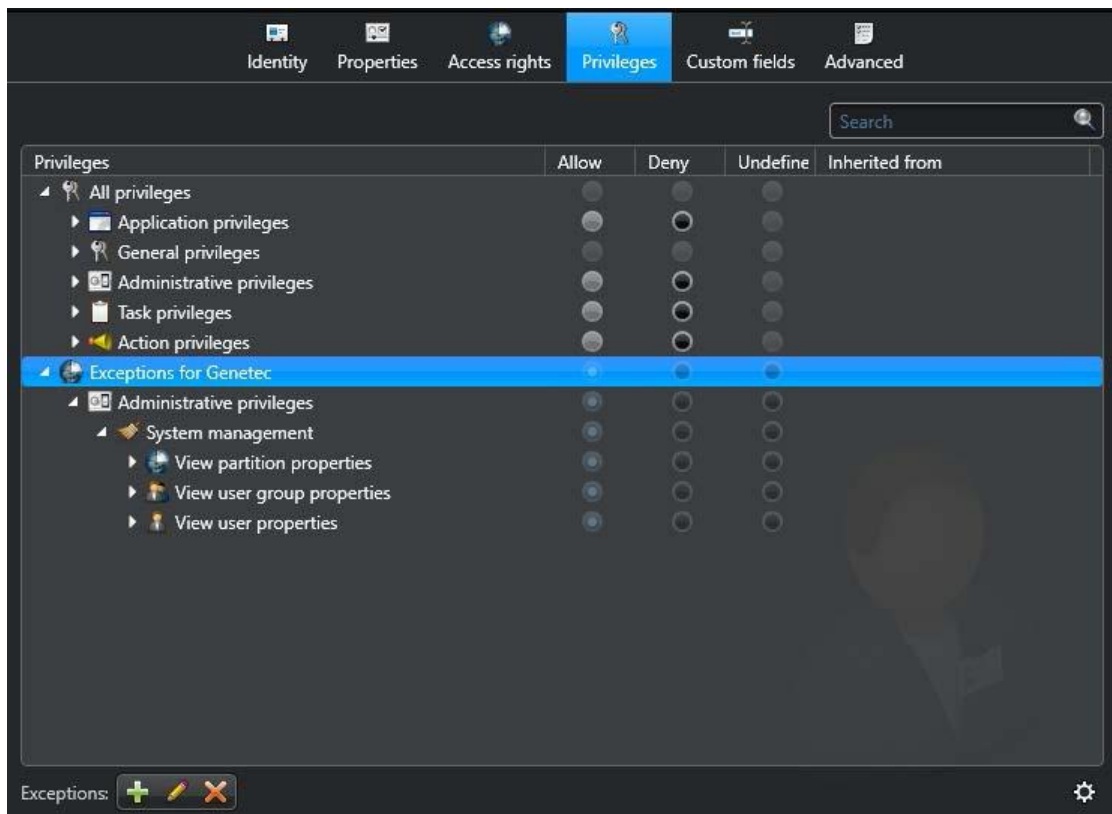


Figure 132. Privileges Exceptions

12. Click **Apply**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 197 of 430

3.11 ADDITIONAL CONFIGURATIONS

This section includes:

[“Areas”](#)

[“Schedule Management”](#)

[“Event Handling”](#)

[“Zones”](#)

[“Advanced Access Control”](#)

[“Badge Designer”](#)

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 198 of 430	

3.11.1 Areas

This section includes:

[“Area View”](#)

[“Area View”](#)

[The area](#) view allows for navigation & searching through commonly used system entities.

Areas

Doors

Cameras

Federated entities

Primarily used by operators in the *Security Desk* but can be useful to Admins as well

Plan Manager Maps are associated with areas. We can structure the map hierarchy using the area view.

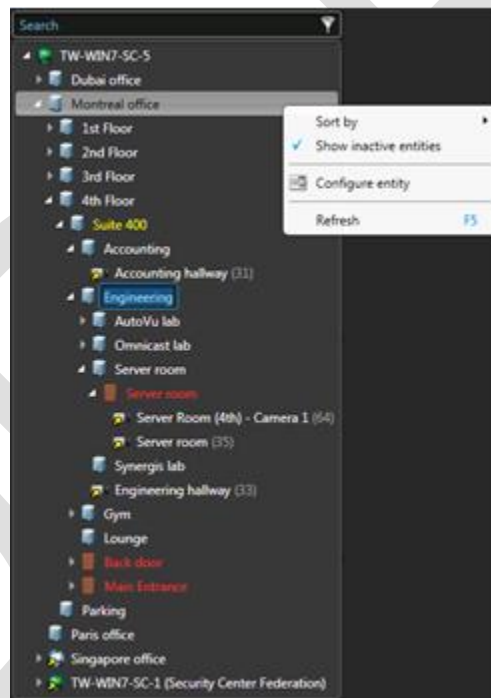


Figure 135. Areas: Area View

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 199 of 430

About the Area View”

[“About Areas”](#)

[“Organizing the Area View”](#)

[“Creating Areas”](#)

DRAFT

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 200 of 430	

An **area** entity represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.

Area activities is a type of investigation task that reports on access control events pertaining to selected areas.

Area presence is a type of investigation task that provides a snapshot of all cardholders and visitors currently present in a selected area.

The **Area view** task is an administration task that allows you to configure areas, doors, cameras, tile plugins, intrusion detection areas, zones, and other entities found in the area view.

The **area view** is a view that organizes the commonly used entities such as doors, cameras, tile plugins, intrusion detection areas, zones, and so on, by areas. This view is primarily created for the day to day work of the security operators.

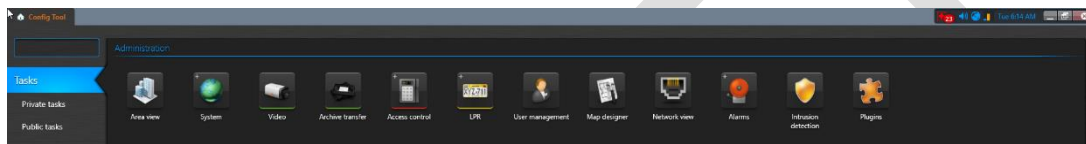


Figure 133. Access Control Configuration: Areas

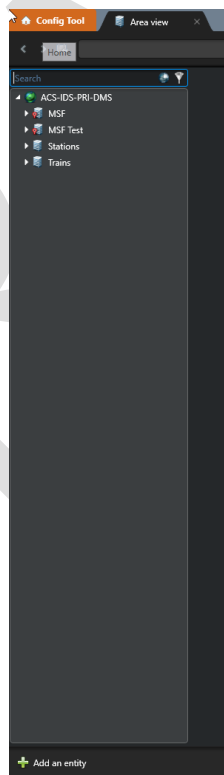


Figure 134. Access Control Configuration: Area View

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 201 of 430

3.11.1.1 Area View

The area view allows for navigation & searching through commonly used system entities.

- Areas
- Doors
- Cameras
- Federated entities

Primarily used by operators in the *Security Desk* but can be useful to Admins as well

Plan Manager Maps are associated with areas. We can structure the map hierarchy using the area view.

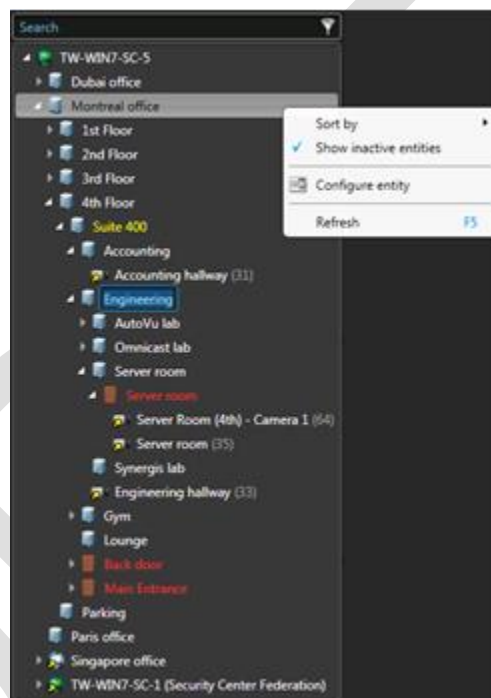


Figure 135. Areas: Area View

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 202 of 430

3.11.1.2 About the Area View

Using the area view, you can find and view all the entities in your system quickly.

The entities in the area view are organized in a hierarchy (or entity tree) according to their logical relationships with areas. For example, the doors leading to an area, and other devices located within the area, such as cameras, are displayed below that area in the hierarchy as child entities.

From the area view, you can do the following:

- Find entities you want to view in the canvas.
- Drag multiple entities from the area view into the canvas.
- Rename local entities.
- Jump to entity configuration pages, if you have the required privileges.

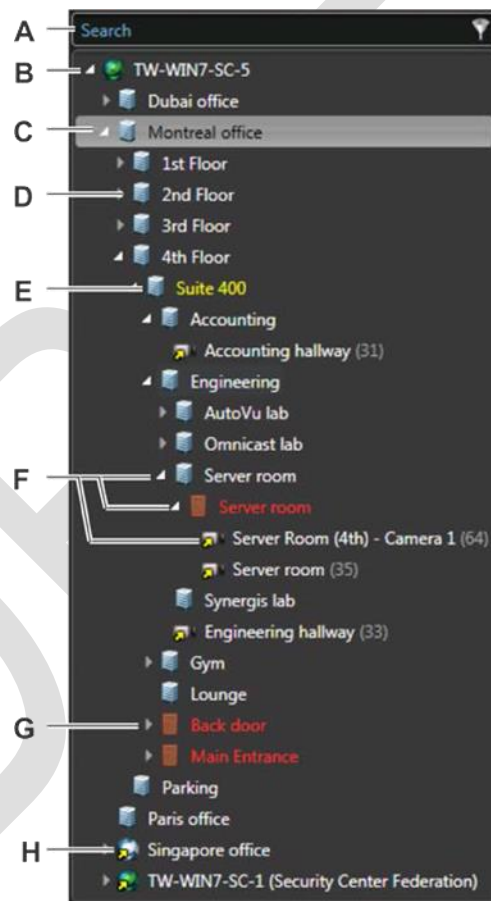


Figure 136. Area View

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 203 of 430

An access rule is a type of entity that defines a list of cardholders to whom access is either granted or denied based on a schedule. An access rule can be applied to a secured area or to an access point.

- A. **Search box** Type in the Search box to find the entities containing that text in their category, name, or description.
- B. **System entity** The system entity (🟢) cannot be viewed in the canvas.
- C. **Additional commands** Right-click an entity in the area view to use additional commands, such as creating or deleting entities, diagnosing the selected entity, launching a report on the selected entity, or refreshing the area view.
- D. **Area entity** Area entities (📍) can represent a concept or physical location. It is a logical grouping.
- E. **Yellow entity** Whenever an entity name is displayed in yellow, it means that there is a problem with the settings.
- F. **Arrow icons** Click the arrows in the entity tree to show or hide child entities.
- G. **Red entity** Indicates that the entity is offline, and the server cannot connect to it, or the server is offline.
- H. **Federated entity** All entities imported from federated systems are shown with a yellow arrow superimposed on the regular entity icon (🟡). They are called federated entities.

3.11.1.3 About Areas

An area entity represents a concept or a physical location (room, floor, building, site, and so on) used for grouping other entities in the system.

You can use areas to group system entities logically or to prevent unauthorized users from viewing selected system entities. A secured area is an area entity that represents a physical location where access is controlled. A secured area consists of perimeter doors (doors used to enter and exit the area) and access restrictions (rules governing the access to the area).

3.11.1.4 Organizing the Area View

As the system administrator, you need to create an area view structure that is easy for everyone to understand and navigate.

You can re-organize the entities in the area view by dragging them to another area, selecting multiple entities at once and drag them to another area, renaming entities, and copying entities. You can also create and delete entities.

NOTE: You cannot edit the names of federated entities.

The way you structure the area view in **Config Tool** is also how it is displayed in *Security Desk*.

To organize the area view:

1. From the **Config Tool** home page, open the **Area view** task.

NOTE: The area view task in Config Tool is the only place where you can change the area view structure. Do not confuse this administrative task with the area view tab found in most investigation tasks available in Security Desk.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 204 of 430

2. To move entities under another area, do one of the following:

- Select an area or entity, and then drag it to a different area.
- Hold the **Shift** key, select multiple entities, and then drag them to a different area.

The selected entities are now a child entities of that area (below that area in the hierarchy).

3. To rename an entity, select the entity, press **F2**, type a new name, and press **ENTER**.

TIP: You can rename any entity from the area view of any task as long as you have the administrative privilege to modify that entity.

4. To copy an entity into another area, hold the **Ctrl** key, and then drag the entity into that area.

A copy of the entity is created under the area. If you copied an area under another area, all its child entities (entities below that area) are also copied.

5. If necessary, create new areas for grouping entities.
6. If necessary, delete entities.

3.11.1.5 Creating Areas

To organize the area view, use areas to group entities based on their logical or physical relationship.

An area is a concept or a physical location (room, floor, building, site, and so on) that is used for the logical grouping of entities in the system.

You can create areas anywhere in the area view hierarchy.

To create an area:

1. Open the **Area view** task.
2. Click a **partition** (🌐) or an **area entity** (📁) you want to create the new area under.
3. Click **Add an entity** (+) > **Area**.
4. Type a name for the area, and press **ENTER**.

After you finish

If you are defining an area for access control, then secure the area.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 205 of 430

3.11.2 Schedule Management

This section includes:

[“Schedules”](#)

[“Create a Schedule”](#)

[“Error! Reference source not found.”](#)

[“Error! Reference source not found.”](#)

[“Configure a Schedule”](#)

[“Specific Schedules”](#)

[“Period Types”](#)

[“About Schedules”](#)

[“About Twilight Schedules”](#)

[“Creating Schedules”](#)

[“Defining Daily Schedules”](#)

[“Defining Weekly Schedules”](#)

[“Defining Ordinal Schedules”](#)

[“Defining Schedules with Specific Dates”](#)

[“Defining Twilight Schedules”](#)

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 206 of 430	

3.11.2.1 Schedules

Schedule defines a set of time constraints that can be applied to many situations, for example:

- When a user is allowed to log on
- When video from a surveillance cameras should be recorded
- When access should be granted to a secured area

3.11.2.2 Create a Schedule

To create a schedule, go to **System task > Schedules**. One schedule exists by default: The Always schedule, it is active 24/7. You can choose from the following options:

- Specific
- Yearly (Ordinal)
- Monthly (Ordinal)
- Weekly
- Daily
- Always (Lowest priority)

3.11.2.3 Configure a Schedule

Each time schedule is represented by:

A date coverage (daily, weekly, recurring dates, or specific dates)

A time coverage (all day, or specific time ranges).

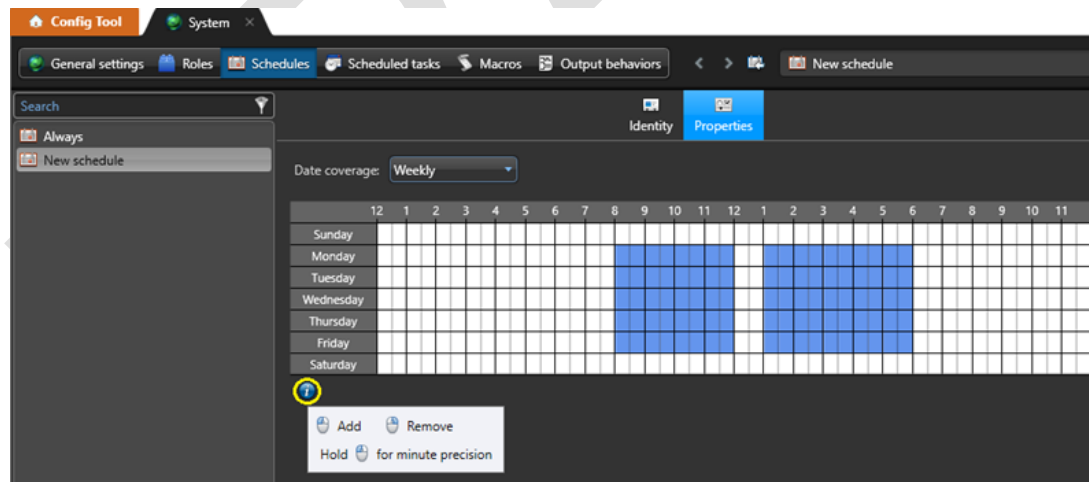


Figure 137. Schedule Management: Configuring a Schedule

3.11.2.4 Specific Schedules

A specific schedule allows you to select specific, non-recurring dates.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 207 of 430

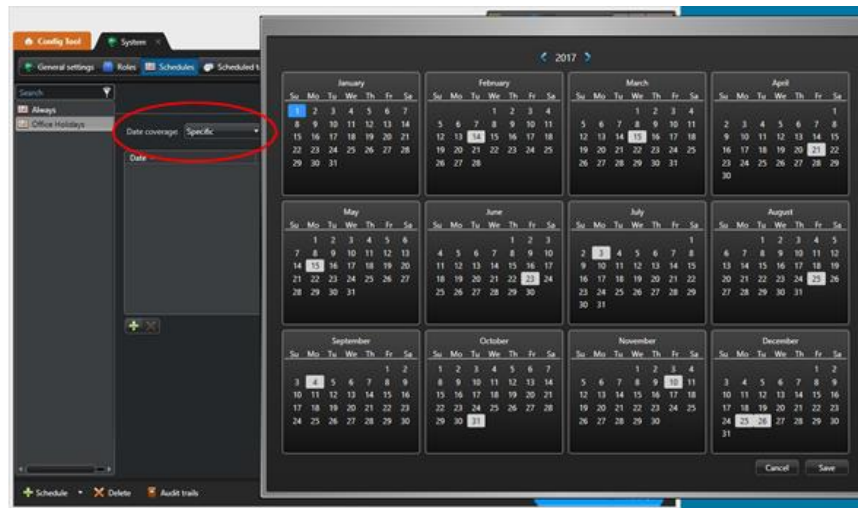


Figure 138. Schedule Management: Specific Schedules

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 208 of 430	

3.11.2.5 Period Types

Schedules can be configured for different “Period Types” like *Daily*, *Weekly*, *Ordinal* and *Specific*.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 209 of 430	

A schedule is a type of entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).

A scheduled task is a type of entity that defines an action that executes automatically on a specific date and time, or according to a recurring schedule.

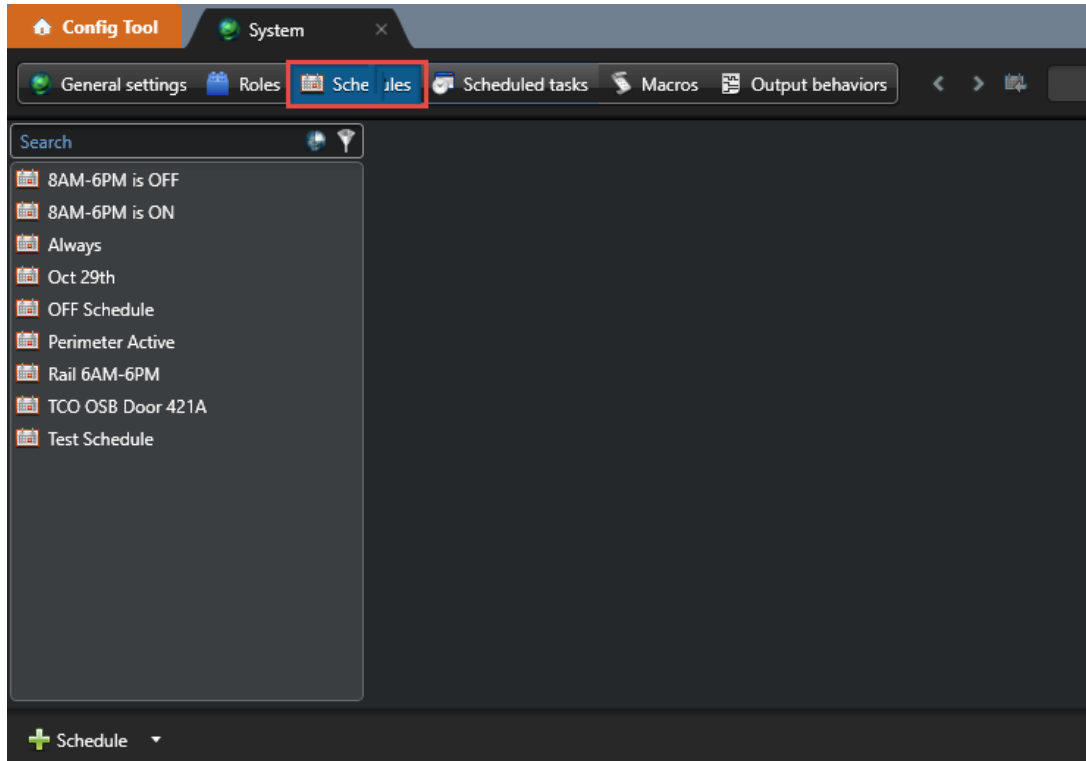


Figure 139. Access Control Configuration: Schedule Management

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 210 of 430

3.11.2.6 About Schedules

A schedule is a type of entity that defines a set of time constraints that can be applied to a multitude of situations in the system. Each time constraint is defined by a date coverage (daily, weekly, ordinal, or specific) and a time coverage (all day, fixed range, daytime, and nighttime).

Each time constraint is characterized by a date coverage (date pattern or specific dates covered by the schedule) and a time coverage (time periods that apply during a 24-hour day).

When the Security Center Directory is installed, the Always schedule is created by default. This schedule has a 24/7 coverage. It cannot be renamed, modified, or deleted, and has the lowest priority in terms of schedule conflict resolution.

Time zones for schedules

The time of day for a schedule is based on the local time zone set in each individual context where it is applied. For example, if the schedule is used to set continuous video recording from 9 a.m. to 5 p.m., whether the video unit is in Tokyo or London, the recording occurs on schedule according to the local time. This is because every video unit has a time zone setting to control video settings and recordings relative to the unit's local time.

When a schedule is applied to an entity that has no time zone settings, such as the logon schedule for a user, the local time is taken from the server hosting the Directory role.

Schedule conflicts

You might have a scheduling conflict when two overlapping schedules are applied to the same function. For example, if two schedules are applied to the recording of the same camera.

Security Center can resolve some of these conflicts by giving priority to the most specific (or restrictive) schedule. The specificity of a schedule is determined by its date coverage option.

The following lists the date coverage options in decreasing order of priority:

1. **Specific** (Runs only once. Highest priority)
2. **Ordinal** (Repeats on a monthly or yearly basis)
3. **Weekly** (Repeats every week)
4. **Daily** (Repeats every day)
5. **Always** (The default schedule. Has the lowest priority)

IMPORTANT: When two overlapping schedules with the same priority level are applied to the same function, you have an unresolved conflict. If the two schedule were applied to an entity, an Entity warning occurs, and the entity with the conflicting configuration is displayed in yellow in the entity browser.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 211 of 430

3.11.2.7 About Twilight Schedules

A twilight schedule is a type of schedule entity that supports both daytime and nighttime coverages. A twilight schedule cannot be used in all situations. Its primary function is to control video related behaviors.

Benefits of twilight schedules

Twilight schedules are designed for situations where the sunlight has an impact on the system's operation, such as video settings and recording. Some typical uses of the twilight schedules are the following:

- To record video only during daytime.
- To boost the video encoder's sensitivity after sunset.
- To disable motion detection during twilight.

Limitations of twilight schedules

Twilight schedules have the following limitations:

- They cannot be used in any situation involving access control entities.
- The entity the schedule applies to must have a geographical location setting, such as video units.
- The **Weekly** option for date coverage is not available.
- The **All day** and **Range** options for time coverage are not available.
- They are not visible in contexts where they are not applicable.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 212 of 430

3.11.2.8 Creating Schedules

To define a set of time constraints for a multitude of situations, such as when a user can log on to the system or when video from a surveillance camera can be recorded, you can create schedules and then apply them to specific entities.

When the *Security Center* Directory is installed, the Always schedule is created by default. This schedule has a 24/7 coverage. It cannot be renamed, modified, or deleted, and has the lowest priority in terms of schedule conflict resolution.

If you want to use schedules for any of your settings in Security Center, you must create the schedules in advance.

To create a schedule:

6. Open the **System task** and click the **Schedules** view.
7. Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.
8. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply**.
9. Click the **Properties** tab.
10. From the **Date coverage** drop-down list, choose one of the following:
 - **Daily**: Defines a pattern that repeats every day.
 - **Weekly**: Defines a pattern that repeats every week. Each day of the week can have a different time coverage. This option is not available for twilight schedules.
 - **Ordinal**: Defines a series of patterns that repeat on a monthly or yearly basis. Each date pattern can have a different time coverage. For example, on July 1st every year, on the first Sunday of every month, or on the last Friday of October every year.
 - **Specific**: Defines a list of specific dates in the future. Each date can have a different time coverage. This option is ideal for special events that occur only once.

NOTE: The Daily, Ordinal, and Specific schedules allow you to define twilight settings.

11. Click **Apply**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 213 of 430

3.11.2.9 Defining Daily Schedules

To define a set of time constraints for situations that occur daily, you can define daily schedules and then apply them to entities.

Time ranges are shown as colored blocks on a time grid. Each block represents 30 minutes. When you click and hold your left mouse button, a pop-up window opens. Each block on the grid represents one minute.

To define a daily schedule:

1. Open the **System** task and click the **Schedules** view.
2. Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply**.
4. Click the **Properties** tab.
5. From the **Date coverage** drop-down list, select **Daily**.
6. From the **Time coverage** drop-down list, select **All day** or **Range**.
7. Using the **time grid**, set the time coverage as follow
 - To select blocks of time, **left-click** your mouse.
 - To remove blocks of time, **right-click** your mouse.
 - To select or remove a successive block of time, click and drag your mouse.
 - To zoom in on the time grid and select specific minutes, click and hold your left mouse button.
8. Click **Apply**.

Example

The following example shows a daily schedule from 6 p.m. to 6 a.m. The time grid shows a 24-hour day in blocks of 30 minutes.

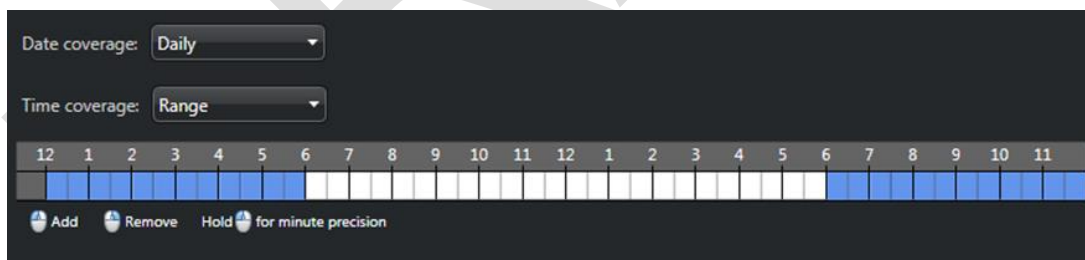


Figure 140. Schedule Management: Daily Schedule

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 214 of 430

3.11.2.10 Defining Weekly Schedules

To define a set of time constraints for situations that occur weekly, you can define weekly schedules and then apply them to entities.

Time ranges are shown as colored blocks on a time grid. Each block represents 30 minutes. When you click and hold your left mouse button, a pop-up window opens. Each block on the grid represents one minute.

To define a weekly schedule:

1. Open the **System** task and click the **Schedules** view.
2. Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply**.
4. Click the **Properties** tab.
5. From the **Date coverage** drop-down list, select **Weekly**.
6. Using the **time** grid, set the time coverage as follows:
 - To select blocks of time, **left-click** your mouse.
 - To remove blocks of time, **right-click** your mouse.
 - To select or remove a successive block of time, click and drag your mouse.
 - To zoom in on the time grid and select specific minutes, click and hold your left mouse button.
7. Click **Apply**.

Example

The following example shows a weekly schedule from 9 a.m. to 5 p.m., from Monday to Friday, with a half-hour break between 12:00 p.m. and 12:30 p.m.

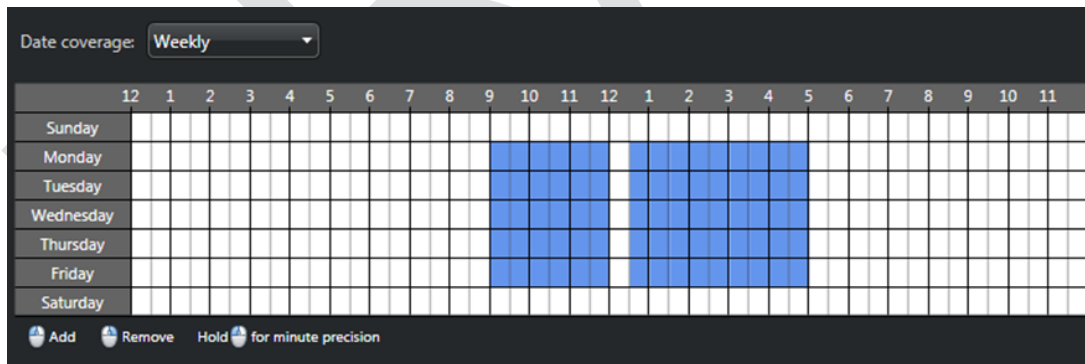


Figure 141. Schedule Management: Weekly Schedule

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 215 of 430

3.11.2.11 Defining Ordinal Schedules

To define a set of time constraints for situations that include a series of repetitive patterns, each with a different time coverage, you can define ordinal schedules and then apply them to entities.

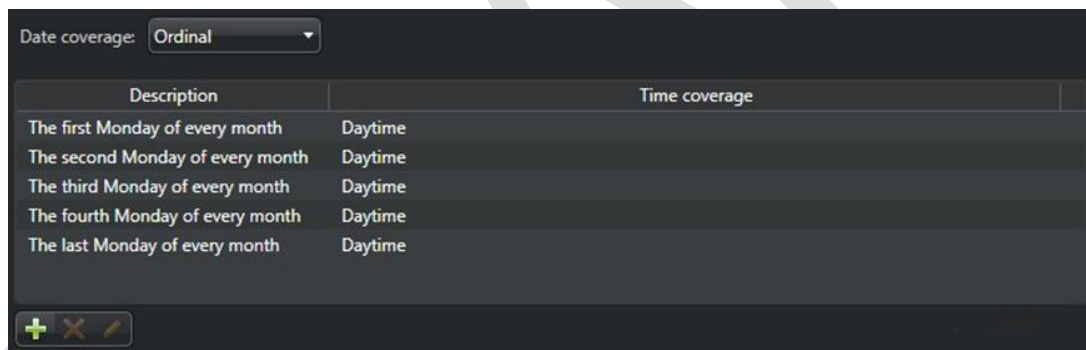
Ordinal schedules are ideal for events that repeat. You can define as many dates as necessary within a single schedule entity.

To define an ordinal schedule:

1. Open the **System** task and click the **Schedules** view.
2. Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply**.
4. Click the **Properties** tab.
5. From the **Date coverage** drop-down list, select **Ordinal**, and then click Add an item (+).
6. Select a day and a month.
7. From the **Time coverage** drop-down list, select **All day**, **Range**, **Daytime**, or **Nighttime** (see [Defining Twilight Schedules](#) for information on daytime and nighttime time coverages).
8. Click **OK** and then click **Apply**.

Example

You can configure something similar to the Weekly pattern using the Ordinal pattern. The following example shows a schedule that cover the daytime of every Monday of the year.



Description	Time coverage
The first Monday of every month	Daytime
The second Monday of every month	Daytime
The third Monday of every month	Daytime
The fourth Monday of every month	Daytime
The last Monday of every month	Daytime

Figure 142. Schedule Management: Ordinal Schedule

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 216 of 430

3.11.2.12 Defining Schedules with Specific Dates

To define a set of time constraints for situations that will occur on specific dates, where each date can have a different time coverage, you can define schedules with specific dates and then apply them to entities.

You can set a different time range for each date in the schedule.

To define a schedule with specific dates:

1. Open the **System** task and click the **Schedules** view.
2. Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply**.
4. Click the **Properties** tab.
5. From the **Date coverage** drop-down list, select **Specific**, and then click **Add an item** ().
6. Select dates on the calendar and click **Close**.
7. Select an entry and, from the **Time coverage** drop-down list, do one of the following:
 - Select **All day**.
 - Select **Range** and then select specific times on the grid for the **Day before**, the **Current day**, or the **Day after**.
 - Select **Daytime** or **Nighttime** (see [Defining Twilight Schedules](#) for information on daytime and nighttime time coverages).
8. Click **Apply**.

Example

The following example shows a specific schedule covering July 1st, 2017 from 9 p.m. the day before to 3 a.m. the day after.

The screenshot shows the 'Schedule Management' interface. At the top, 'Date coverage' is set to 'Specific'. Below it, a 'Date' field shows '01/07/2017' and a 'Time coverage' field shows 'Multiple time range: Day before: 21:00:00 - 24:00:00 | Current day: 00:00:00 - 24:00:00 | Day after: 00:00:00 - 03:00:00'. Below this is a 'Time coverage' dropdown set to 'Range' and a grid for selecting time ranges for 'Day before', 'Current day', and 'Day after'. The grid has columns for hours 12, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. The 'Day before' row shows a blue bar from 21:00:00 to 24:00:00. The 'Current day' row shows a blue bar from 00:00:00 to 24:00:00. The 'Day after' row shows a blue bar from 00:00:00 to 03:00:00. At the bottom, there are 'Add', 'Remove', and 'Hold for minute precision' buttons.

Figure 143. Schedule Management: Specific Dates

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 217 of 430

3.11.2.13 Defining Twilight Schedules

To define a set of time constraints for situations that cover either daytime or nighttime, where the calculation of exactly when the sun rises and sets is based on a geographical location (latitude and longitude), you can define twilight schedules.

Twilight schedules are designed for situations where the sunlight has an impact on the system's operation, such as with video settings and video recording.

To define a twilight schedule:

1. Open the **System** task and click the **Schedules** view.
2. Click **Schedule** (+), type a name for the schedule, and then press **ENTER**.
3. In the **Identity** tab, enter basic properties of the schedule, and then click **Apply**.
4. Click the **Properties** tab.
5. From the **Date coverage** drop-down list, select **Daily**, **Specific**, or **Ordinal**.
6. If you selected **Specific** or **Ordinal**, set up the date coverage.
7. From the **Time coverage** drop-down list, select **Daytime** or **Nighttime**.
8. Select the **Sunrise** or **Sunset** options, and then select the amount of time to offset the sunrise time or sunset time (up to 2 hours before or after).

Example

The following example shows a daily schedule using a Daytime coverage. The time coverage starts 10 minutes after the sun rises and ends 10 minutes before the sun sets.

The screenshot shows a configuration window for a twilight schedule. It includes the following fields and options:

- Date coverage:** A dropdown menu set to "Daily".
- Time coverage:** A dropdown menu set to "Daytime".
- Offsets:** Two rows of controls.
 - The first row is for "Sunrise" (checked) with a "Minus" dropdown, a "0" hour(s) spinner, and a "10" minute(s) spinner.
 - The second row is for "Sunset" (checked) with a "Minus" dropdown, a "0" hour(s) spinner, and a "10" minute(s) spinner.
- Footer:** A blue information icon followed by the text: "Twilight schedules are primarily used for video related functions. They are not visible in contexts where they are not applicable."

Figure 144. Schedule Management: Defining Twilight Schedules

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 218 of 430

3.11.3 Event Handling

This section includes:

[“Event Handling”](#)

[“Security Center Actions”](#)

[“Configuring Event Handling”](#)

[“Event Handling”](#)

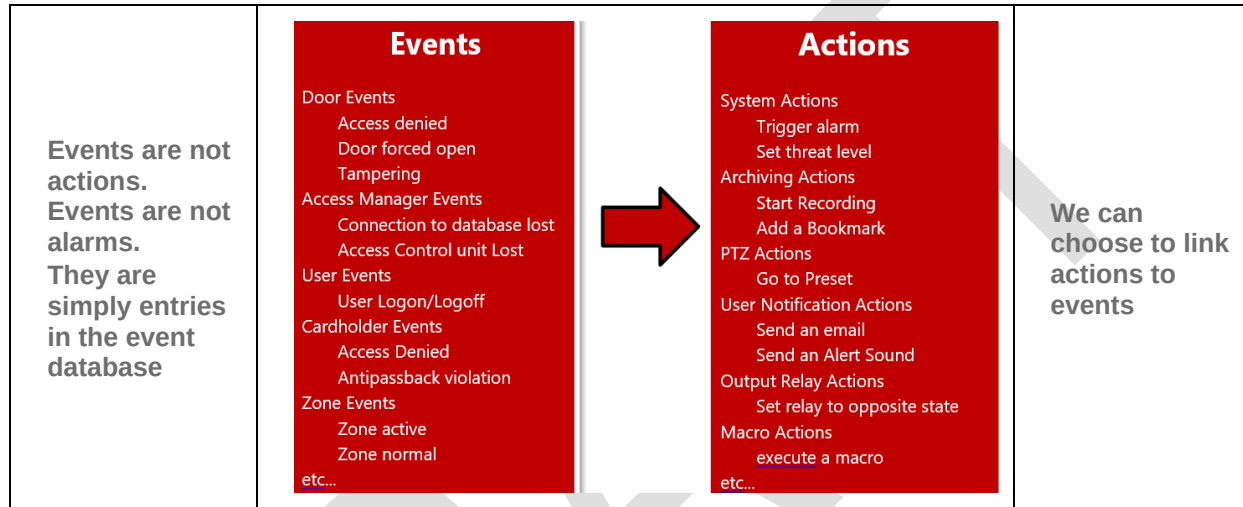


Figure 146. Event Handling: Events to Actions

3.11.3.1 Security Center Actions

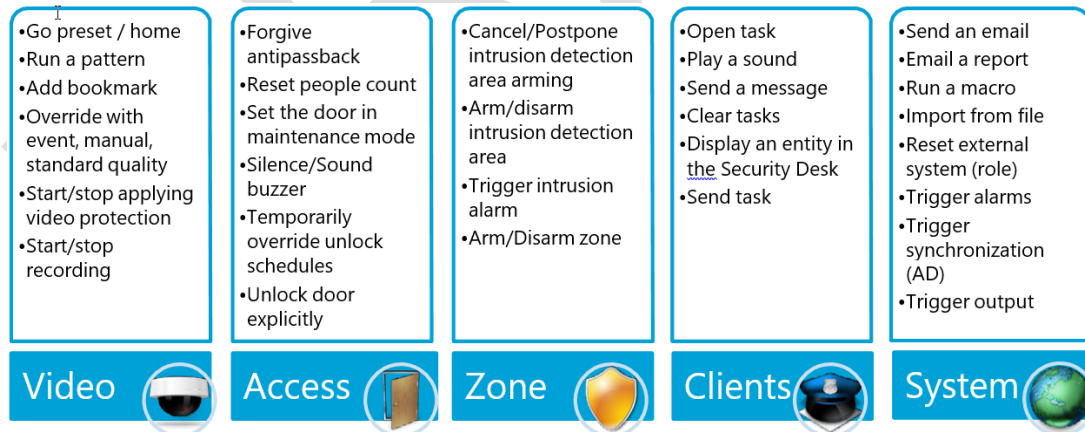


Figure 147. Event Handling: Security Center Actions

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 219 of 430

3.11.3.2 Configuring Event Handling

Actions can be linked to events using Security Center's built-in event handling mechanism:

Config Tool > Source entity > Identity page.

or,

Config Tool > System task > General > Actions tab.

The screenshot shows a configuration window titled "Event-to-action". It contains three main sections, each highlighted with a blue border:

- Event Section:**
 - When: Input active
 - From: Input 3
- Action Section:**
 - Action: Trigger alarm
 - Alarm: Fire escape
- Schedule Section:**
 - Effective: Always

At the bottom right, there are two buttons: "Cancel" and "Save".

Figure 148. Event Handling: Event to Action

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 220 of 430

Monitoring Events”

[“Selecting Events to Monitor”](#)

[“Selecting Entities to Monitor”](#)

[“Event Colors”](#)

[“Creating Custom Events”](#)

[“Creating Custom Events](#)

[You](#) can create your own custom *Security Center* events that you can use for event-to-actions.

Custom events allow you to give descriptive names to standard events generated by input signals from zones, intrusion panels, and so on. They are used to configure custom event-to-actions.

For example, you can associate an input state (normal, active, trouble) of a zone entity to a custom event that describes what is happening, such as Illegal entry or Door open too long for this zone. When this custom event is received in Security Desk, it can trigger an action, using event-to-actions.

To create a custom event:

1. Open the **System** task, click the **General settings** view, and click the **Events** page.
2. Click **Add an item** (+).
3. In the **Create custom event** dialog box, type a **Name** for the new event.
4. From the **Entity type** drop-down list, select the entity type that triggers this event.
5. In the **Value** field, type a unique number to identify the custom event from other custom events. These values are not related to the logical IDs of entities.
6. Click **Save** > **Apply**.

Customizing Monitoring Task Options”

[“Event Occurrence Period”](#)

[“Monitoring Events On Remote Security Desks”](#)

[“Configuring Event/Action”](#)

[“Creating Event-to-Actions”](#)

[“Adding Conditions When Creating Event-to-actions for Video Analytics Events”](#)

[“Elements Used in Event-to-action Conditions for Video Analytics Events”](#)

[“Modifying Event-To-Actions”](#)

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 221 of 430

DRAFT

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 222 of 430	

An event indicates the occurrence of an activity or incident, such as access denied to a cardholder or motion detected on a camera. Events are automatically logged in *Security Center* and can be programmed to trigger actions. Every event mainly focuses on one entity, called the event source.

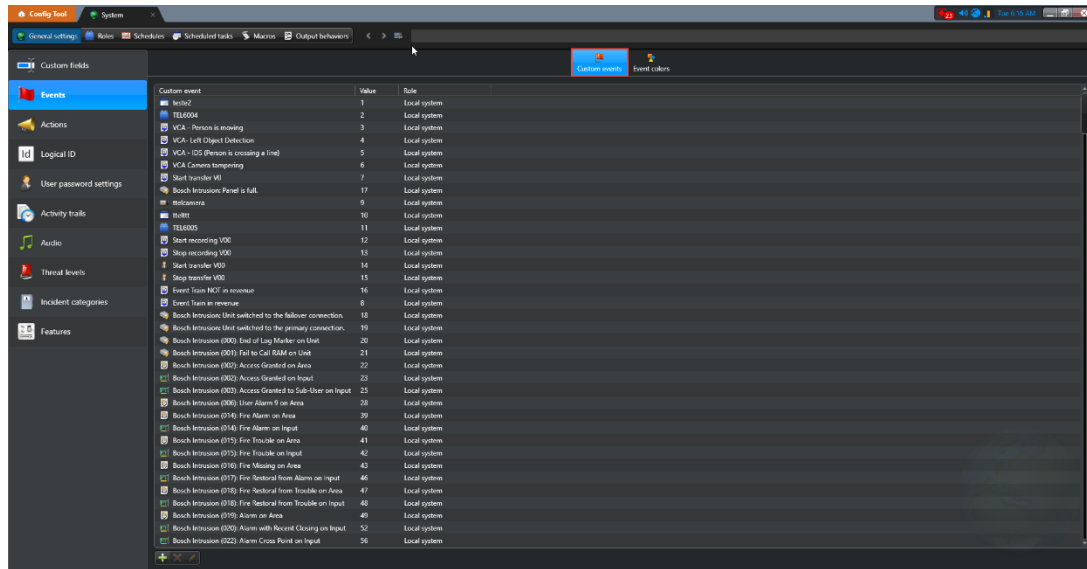


Figure 145. Access Control Configuration: General Settings: Event Handling

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 223 of 430	

3.11.3.3 Event Handling

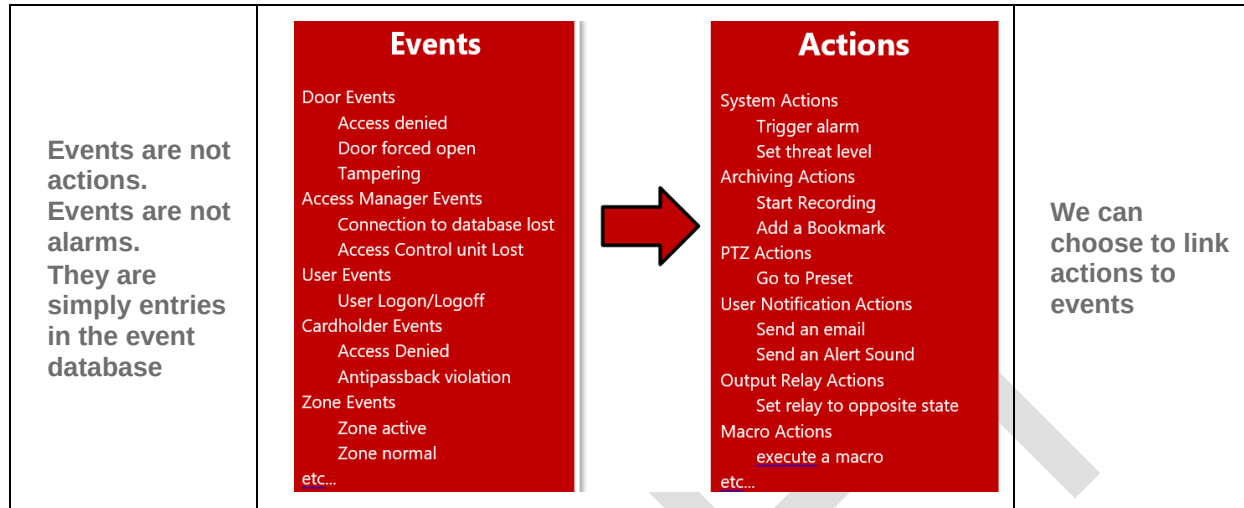


Figure 146. Event Handling: Events to Actions

3.11.3.4 Security Center Actions

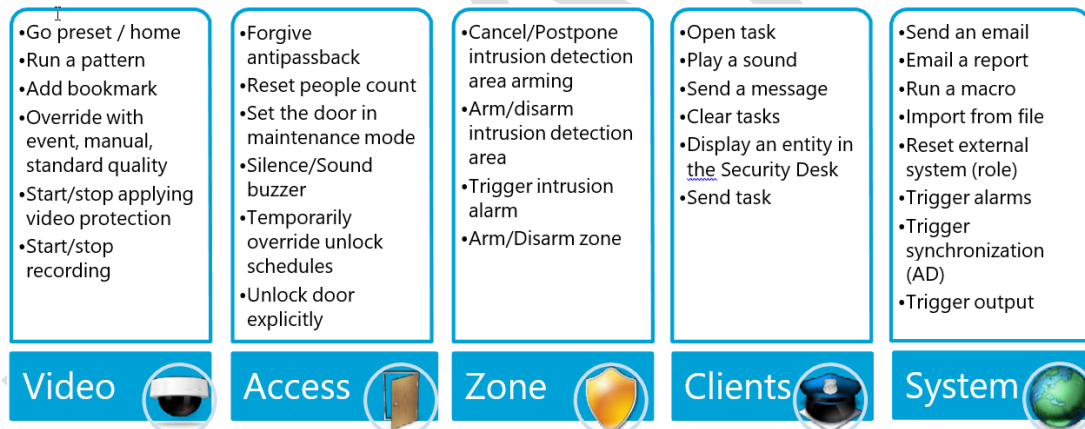


Figure 147. Event Handling: Security Center Actions

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 224 of 430

3.11.3.5 Configuring Event Handling

Actions can be linked to events using Security Center's built-in event handling mechanism:

Config Tool > Source entity > Identity page.

or,

Config Tool > System task > General > Actions tab.

The screenshot shows the 'Event-to-action' configuration window. It has a dark background with blue borders around the input fields. The 'Event' section is at the top, followed by the 'Action' section, and the 'Schedule' section at the bottom. The 'When' field is set to 'Input active' and the 'From' field is set to 'Input 3'. The 'Action' field is set to 'Trigger alarm' and the 'Alarm' field is set to 'Fire escape'. The 'Effective' field is set to 'Always'. There are 'Cancel' and 'Save' buttons at the bottom right.

Figure 148. Event Handling: Event to Action

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 225 of 430

3.11.3.6 Monitoring Events

Using the **Monitoring** task, you can monitor events such as access control events from doors and cardholders, and camera related events, in real time.

When monitoring events, you are actually monitoring the entities that trigger those events. The entities are selected in the Monitoring task. You can customize how the Monitoring task displays information to suit the purpose of the task. For example, if you are monitoring cameras, you can hide everything else except for the canvas tiles to make the camera images bigger. You can create multiple **Monitoring** tasks to monitor different sets of entities (for example, just cameras or doors).

To monitor events:

1. Select the events to monitor.
2. Select the entities that are linked to the events you want to monitor.
Once the entities are selected, events that occur in your system appear chronologically in the event list and in real time. You cannot change the order of the events.
3. To show the **event** list, from the top of the **Monitoring task** window, drag the four gray dots downwards.
4. To choose what event information to display in the event list, **right-click** on a **column heading**, and then click **Select columns** to choose the information you want to display in the list.
Example: In access control systems, you might only want to view cardholder and credential fields.
5. To clear the **event** list, click **Clear event list** (🗑️) in the upper-right corner of the **Monitoring** task.
6. To monitor events in the canvas, choose one of the following two modes:
 - **Tile mode:** Tile mode is the *Security Desk* canvas operating mode where the main area of the canvas is used to display the tiles and the dashboard. In this mode, you can turn monitoring on or off for each tile.
 - **Map mode:** Map mode is a *Security Desk* canvas operating mode where the main area of the canvas is used to display a geographical map, for the exclusive purpose of showing LPR events. You can view LPR events in the map.
7. From the area view, select the entities you want to view in the canvas by dragging them into the canvas.

You can select multiple entities and drag them onto the canvas all at once.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 226 of 430

8. (Optional) To protect the content in the tile from being overwritten by new events, turn off monitoring for that tile as follows:

TIP: This is helpful if you have a tile plugin displayed in the canvas, and do not want it to be replaced by an event.

- A. Select a tile in the canvas.
- B. In the **tile** widget, click **Monitoring** (🔍), and click **Monitor** events.

The checkmark beside **Monitor** events disappears and tile **ID background** turns black.

3.11.3.7 Selecting Events to Monitor

Before you can use the **Monitoring** task, you must select the event types you want to monitor.

To select events to monitor:

1. From the home page, click **Options > Events**.
2. In the **Event options** page, select which events to monitor.
3. In the **Display in tile** column, select the check boxes of the events you want to view in the **Monitoring task** canvas. If the check box is cleared, the event only appears in the event list.
4. Click **Save**.

After you finish

Select the entities you want to monitor that trigger the event types you selected.

3.11.3.8 Selecting Entities to Monitor

Before you can monitor events in the **Monitoring** task, you must select the entities that trigger those events.

Select the events to monitor.

To monitor events, it is important to select which entities you want to monitor, because some event types can be generated by multiple entities. For example, an Access granted event can be generated by a cardholder, visitor, or credential. If you only monitor cardholders, you will not receive all Access granted events.

To select entities to monitor:

1. From the home page, click **Tasks > Monitoring**.
2. (Optional) To give the tab a unique name, right-click the tab, click **Rename** task; in the **Task name** box, type a name, then click **Rename**.

Example: You can rename the tab to indicate what is being monitored; for example, Monitoring camera events. This is helpful when you have multiple monitoring tabs open at the same time.

3. In the **area view**, select the entities you want to monitor (specific cameras, doors, cardholder, and so on).

To select multiple entities, hold **CTRL** or **SHIFT**, and then select the entities.

4. Drag the selected entities over the **Monitoring** (🔍) icon at the bottom of the **Monitoring** task.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 227 of 430

The entities you selected are added to the **Event monitoring** list.

NOTE: By default, all tiles are armed to monitor events. You can arm and disarm all tiles at any time by clicking (🔒). When a tile is armed to monitor events the tile **ID background** is blue.

5. (Optional) To add more entities from the **Event monitoring** dialog box, do the following:
 - A. Click **Monitoring** (🔍), and then under **Event monitoring** click **Add** (+).
 - B. Select the entity type you want to monitor (area view, cardholder, cardholder group, visitor, hotlist, permit, user, asset, and so on).

TIP: Certain entity types, such as areas, doors, zones, and so on, only appear in the area view drop-down list.

- C. Select the entities you want to monitor (specific cameras, doors, cardholder, and so on).
- D. To add a conditional filter, select an entity from the **For** drop-down list.

Example: You can monitor events for a cardholder group at a specific door.

NOTE: Only events that are related to the cardholder group and the door are monitored. You will not receive other events for the door unless you are also monitoring that door.

- E. Click **Add**.

6. (Optional) In the **Tile** column of the **Event monitoring** list, select a tile to display the entity in.

You can associate more than one entity to the same tile. By default, events are displayed in any tile (All).

Example: You can set Tile 1 to display events happening at the *Main Entrance* door.

Monitoring is turned on in the canvas tiles. When a new event occurs, *Security Desk* displays the event in an empty tile. When there are no more empty tiles, the entity that has been displayed for the longest time is replaced by the new event.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 228 of 430

3.11.3.9 Event Colors

When you are monitoring entities, events generated by the entity are displayed in the canvas using different colors, depending on the event type. When you have a large system, this helps you focus on the events that are more important.

Event colors are configured in Config Tool. For more information about assigning colors for events, see the *Security Center Administrator Guide*.

The following figure shows four access control events that have been assigned different colors.

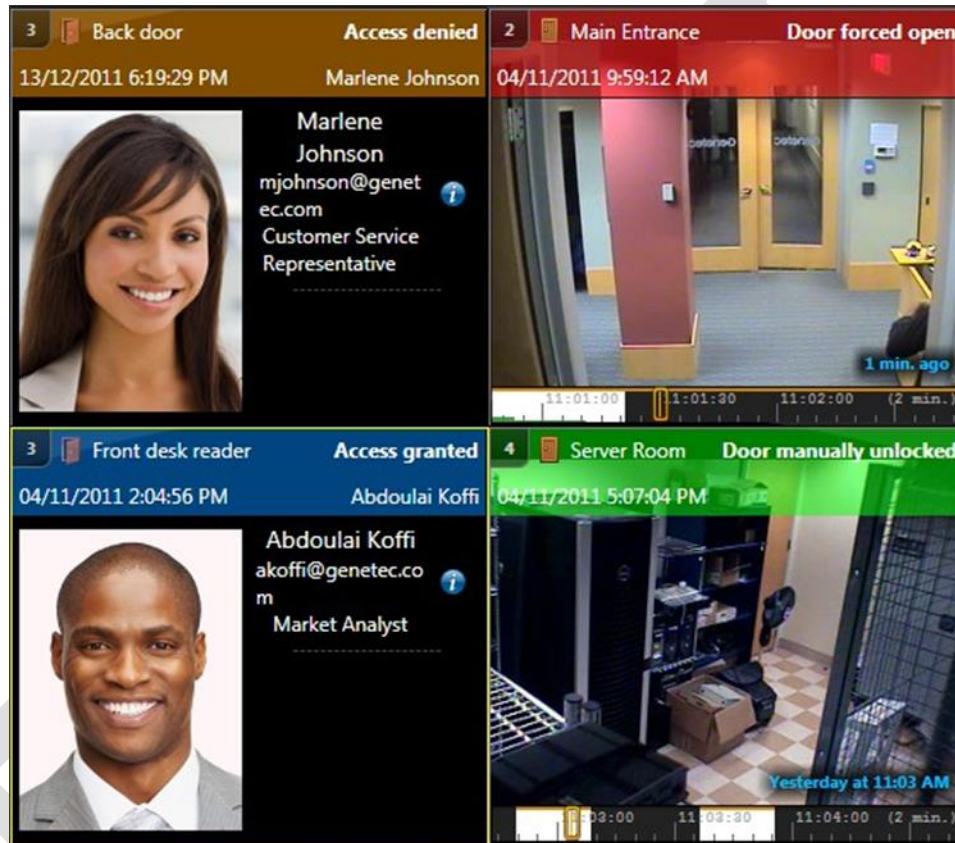


Figure 149. Event Handling: Event Colors

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 229 of 430

3.11.3.10 Creating Custom Events

You can create your own custom *Security Center* events that you can use for event-to-actions.

Custom events allow you to give descriptive names to standard events generated by input signals from zones, intrusion panels, and so on. They are used to configure custom event-to-actions.

For example, you can associate an input state (normal, active, trouble) of a zone entity to a custom event that describes what is happening, such as Illegal entry or Door open too long for this zone. When this custom event is received in Security Desk, it can trigger an action, using event-to-actions.

To create a custom event:

7. Open the **System** task, click the **General settings** view, and click the **Events** page.
8. Click **Add an item** (+).
9. In the **Create custom event** dialog box, type a **Name** for the new event.
10. From the **Entity type** drop-down list, select the entity type that triggers this event.
11. In the **Value** field, type a unique number to identify the custom event from other custom events. These values are not related to the logical IDs of entities.
12. Click **Save > Apply**.

3.11.3.11 Customizing Monitoring Task Options

You can customize how many events are retrieved from the database and displayed when you load a saved **Monitoring** task.

This setting is saved as part of your user profile.

To customize Monitoring task options:

1. From the home page, click **Options > Performance**.
2. In the **Maximum number of events to show** option, select the maximum number of events to load.
3. Click **Save**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 230 of 430

3.11.3.12 Event Occurrence Period

The event occurrence period applies to access control units and intrusion detection units that were temporarily offline. If a unit is offline in *Security Center*, but still physically running, when the unit is re-connected the events that were stored on the unit while it was offline are received in Security Desk. The occurrence period value indicates how long ago the event occurred before the unit came back online and determines what happens when the event is received.

Only certain types of units (for example, HID VertX units) keep a record of events that occur while it is offline.

The four event occurrence values are listed below, with a description of what happens when *Security Center* receives the event:

Online: The event occurred when the unit was online.

Grace period: The event occurred less than 15 minutes before the unit came back online. Security Center treats the event as a normal event. It appears in the event list in the Monitoring task. Actions that are associated with the event using event-to-actions are triggered.

Alarm grace period: The event occurred in between 16 minutes and 72 hours before the unit came back online. When the event is received in Security Center, it does not appear in the event list in the Monitoring task. The only actions that are triggered using event-to-actions are Trigger alarm and Add bookmark. The event is recorded in the database and is available for reporting.

Pre-alarm offline period: The event occurred more than 72 hours before the unit came back online.

When the event is received in *Security Center*, it is only recorded in the database for reporting.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 231 of 430

Reasons why units can be offline

An access control or intrusion detection unit can be offline in *Security Center* for the following reasons:

The unit is rebooting.

The unit's firmware is being upgraded.

The connection between the unit and the Access Manager or Intrusion Manager is lost.

The connection between the Access Manager or the Intrusion Manager and the Directory is lost. When this happens, the role disconnects from its units until the connection with the Directory is re-established.

3.11.3.13 Monitoring Events On Remote Security Desks

In the **Monitoring** task on the remote *Security Desk*, you can use a subset of the actions available to you in a local **Monitoring** task. For example, you can only monitor video and access control and video entities (cameras, areas, doors, intrusion detection areas, and so on).

Connect to one or more *Security Desks* remotely.

To monitor events on remote *Security Desks*:

1. Open the **Monitoring** task.

If the remote workstation does not have a **Monitoring** task open, proceed as follows:

- A. **Right-click** the **Home** tab and click **New task** (+).
- B. Click **Monitoring** and type a name for the task.
- C. Click **Create**.

2. Select which entities to monitor

This is done the same way as in a local **Monitoring** task.

3. To view an entity in a canvas tile, drag or double-click the entity from the area view.

The entity is displayed in your local **Remote** task, and on the remote workstation.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 232 of 430

3.11.3.14 Configuring Event/Action

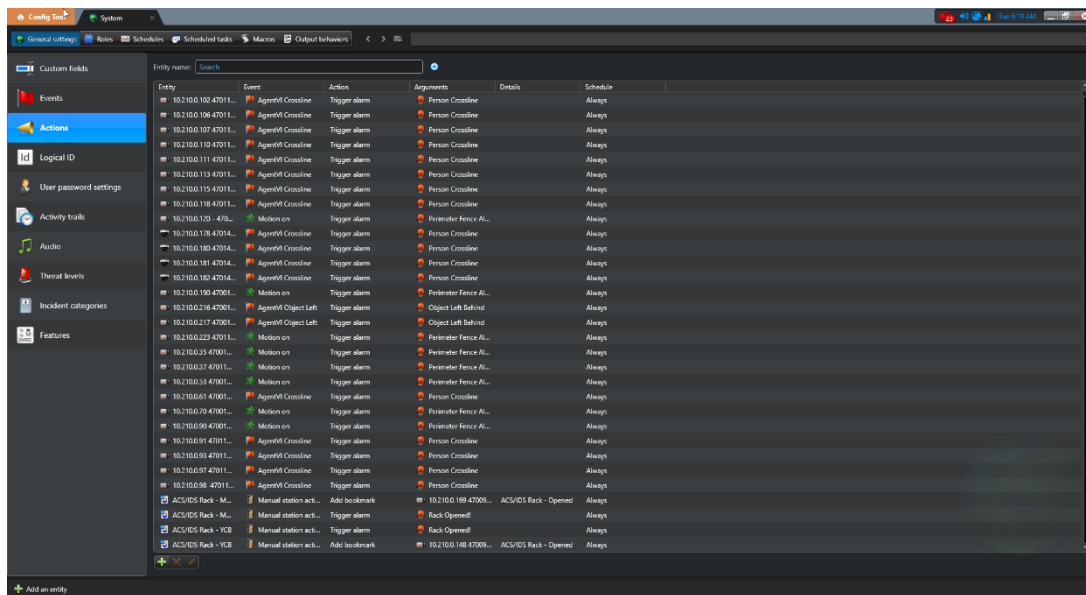


Figure 150. Access Control Configuration: General Settings: Configuring Event/Action

3.11.3.15 Creating Event-to-Actions

If you want certain events that occur in your system to automatically trigger an action, such as sounding an alarm or recording a camera, you can create event-to-actions.

An event-to-action links an action to a particular event. For example, you can configure Security Center to trigger an alarm when a door is forced open.

To create an event-to-action:

1. Open the **System** task and click **General settings** view.
2. Click the **Actions** page and click **Add an item** ().
3. From the **When** drop-down list in the **Event-to-action** dialog box, select an **event** type.
 - A. (Optional: Camera events only) If you select camera video analytics events, you can specify a condition for camera analytics events. For example, **Face detected**, or **Face recognized**.
 - B. (Optional: *Custom events* only) If you select a *custom event*, you can specify a text string in the and field which must be included in the macro that triggers the event-to-action.
4. In the **From** option, click **Any entity**, and then select an entity that triggers the event.

By default, the *event-to-action* occurs when any entity triggers the event type you select. If you select a specific entity, then you might have to set other parameters (for example, if you select a door, then you must also select a door side).
5. From the **Action** drop-down list, select an action type and configure its parameters.

For example, if you select the **Send an email** action, you can create an email template message that can include fields that are related to the report or event. In this case, using the

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 233 of 430

{CardholderName} field, you could create the message: Unauthorized access attempt by {CardholderName}.

6. In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.

If the event occurs outside of the defined schedule, then the action is not triggered. For example, you might want to sound an alarm only when a window is opened during the weekend. By default, **Always** is selected.

7. Click **Save**.

The **Save** button is only available when all the arguments required by the event-to-action type are specified.

The new event-to-action is added to the list of system actions.

3.11.3.16 Adding Conditions When Creating Event-to-actions for Video Analytics Events

When creating event-to-actions for video analytics events, you can specify additional conditions based on camera analytics to trigger an action. For example, you can specify that an action occurs only when the direction of travel is right, or the vehicle is traveling at a particular speed.

Ensure that video analytics is enabled and configured for your cameras.

Familiarize yourself with the video analytics event types.

Conditions must be typed as an expression that contains an identifier, an operator, and a value (not case sensitive). For example, [RuleName] = "RuleA". To know more about the operators and identifiers that can be used, [see Elements used in event-to-action conditions for video analytics events on page 202.](#)

Identifiers must be typed in square brackets: [RuleName].

Text values must be typed in quotation marks: "ABC123".

You can use AND and OR to combine multiple expressions. When doing this, use parentheses to force the order of the evaluation. For example, if you type ([Count] > 20 AND [Update] = "Punctual") OR ([Count] > 50 AND [Direction] = "right") the AND operator takes precedence.

You can use the exclamation point (!) to exclude an expression. For example, if you type [RuleName] contains "RuleA" AND !([Update] = "punctual"), any camera with a rule name that contains the value "RuleA" and an update other than "punctual" will trigger an action.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 234 of 430

Camera analytics are not generated 100% of the time. An event-to-action might not be processed if the camera is unable to generate the analytic specified in the condition. For example, if the condition is [Count] > 50 and the camera cannot produce a value for count, *Security Center* will evaluate the condition as being false and the action will not be processed.

To add a condition when creating an event-to-action for a video analytics event:

1. Open the **System** task and click **General settings** view.
2. Click the **Actions** tab and click **Add an item** (+).
3. From the **When** drop-down list in the **Event-to-action** dialog box, select a video analytics event from the **event** list.
4. Click **Specify a condition** and type the expression.

TIP: Hover your mouse over the field for examples of valid expressions. The field will appear in red if the expression you enter is invalid.

5. In the **From** drop-down list, leave the default **Any entity** unchanged.
6. From the **Action** drop-down list, select an action type and configure its parameters.
For example, if you select **Send an email**, then you must also select the email recipients.
7. In the **Effective** option, click **Always**, and select a schedule when the event-to-action is active. If the event occurs outside of the defined schedule, then the action is not triggered.
8. Click **Save**.

The **Save** button is only available when all the arguments required by the event-to-action type are specified.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 235 of 430

3.11.3.17 Elements Used in Event-to-action Conditions for Video Analytics Events

If you add a condition when creating an event-to-action for a video analytics event, the condition must contain an identifier, an operator, and a value (text or numeric).

Operators

The following table lists operators that can be used and the corresponding value types, descriptions, and examples.

Table 34. Event-to-Action Conditions

Operator	Description	Type of Value	Example
>	Greater than the specified value.	Numeric	[Count] > 80
<	Less than the specified value.	Numeric	[Count] < 75
>=	Greater than or equal to the specified value.	Numeric	[Count] > 80
<=	Less than or equal to the specified value.	Numeric	[Count] < 75
=	Equal to the specified value.	Numeric	[Count] = 80
		Text	[Direction] = "left"
StartsWith	Starts with the specified value.	Text	[RuleName] startsWith "X"
endsWith	Ends with the specified value.	Text	[RuleName] endsWith "C"
contains	Contains the specified value.	Text	[RuleName] contains "Rule123"
matches	Respects the regular expression.	Text	[RuleName] matches "regularExpression" expression1 OR expression2 AND expression3

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 236 of 430

Identifiers

The following table lists the common identifiers that can be used and the corresponding value types, descriptions, and examples.

IMPORTANT: These identifiers are only supported for people counter events (Object count reached and Object count changed).

Table 35. Event-to-Action Identifiers

Operator	Description	Type of Value	Example
RuleName	The rule name configured on the device.	Text	[RuleName] contains "RuleA"
Update	Update values are punctual or summary.	Text	[Update] = "punctual"
Direction	Direction values are in, out, left, or right.	Text	[Direction] = "right"
Count	Numeric value.	Numeric	[Count] > 2

For more information about specifying conditions when creating event-to-actions for camera analytics events, see [Adding Conditions When Creating Event-to-actions for Video Analytics Events](#).

3.11.3.18 Modifying Event-To-Actions

If you need to modify an event-to-action, but you have a long list of them in Security Center, you can search for them using a combination of source entity (name and type), event type, and action type.

To modify an event-to-action:

- Open the **System** task and click **General settings** view.
- Click the **Actions** page, and **Advanced search** (🔍) to show the search filters, and filter out the event-to- actions as follows:
 - Entity name:** Search for source entity names starting with the search string.
 - Entity type:** Select a specific source entity type (default=All).
 - Event:** Select a specific event type (default=All).
 - Action:** Select a specific action type (default=All).
- Select an event-to-action and click **Edit the item** (✎).
- From the **When** drop-down list in the Event-to-action dialog box, select an event type.
 - (Optional: Camera events only) If you select camera video analytics events, you can specify a condition for camera analytics events. For example, **Face detected**, or **Face recognized**.
 - (Optional: Custom events only) If you select a custom event, you can specify a text string in the and field which must be included in the macro that triggers the event-to-action.
- In the **From** option, click **Any entity**, and then select an entity that triggers the event.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 237 of 430

By default, the event-to-action occurs when any entity triggers the event type you select. If you select a specific entity, then you might have to set other parameters (for example, if you select a door, then you must also select a door side).

6. From the **Action** drop-down list, select an action type and configure its parameters.

For example, if you select the **Send an email** action, you can create an email template message that can include fields that are related to the report or event. In this case, using the **{CardholderName}** field, you could create the message: Unauthorized access attempt by {CardholderName}.

7. In the **Effective** option, click **Always**, and select a schedule when this event-to-action is active.

If the event occurs outside of the defined schedule, then the action is not triggered. For example, you might want to sound an alarm only when a window is opened during the weekend. By default, **Always** is selected.

8. Click **Save**.

The **Save** button is only available when all the arguments required by the event-to-action type are specified.

9. To delete an event-to-action, select the item, and click **Delete ()**.

10. Click **Apply**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 238 of 430

3.11.4 Zones

This section includes:

[“About Zones”](#)

[“I/O Linking”](#)

[“Hardware Zones”](#)

[“Virtual Zones”](#)

[“I/O Zones”](#)

[“I/O Linking Example”](#)

[“Global I/O: Peer-to-Peer Communication on SCL”](#)

[“Peer to Peer SCL Communications”](#)

[“Global I/O; Peer to Peer Setup”](#)

[“Global I/O; Peer to Peer Configuration”](#)

[“I/O Zone Properties”](#)

[“I/O Zone Limitations”](#)

[“Differences between the Types of Zone”](#)

[“About Zone Managers”](#)

[“About Output Behaviors”](#)

[“Creating Hardware Zones”](#)

[“Configuring Hardware Zone Settings”](#)

[“Creating Virtual Zones”](#)

[“Configuring Virtual Zone Settings”](#)

[“Creating I/O Zones”](#)

[“Configuring I/O Zone Settings”](#)

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 239 of 430

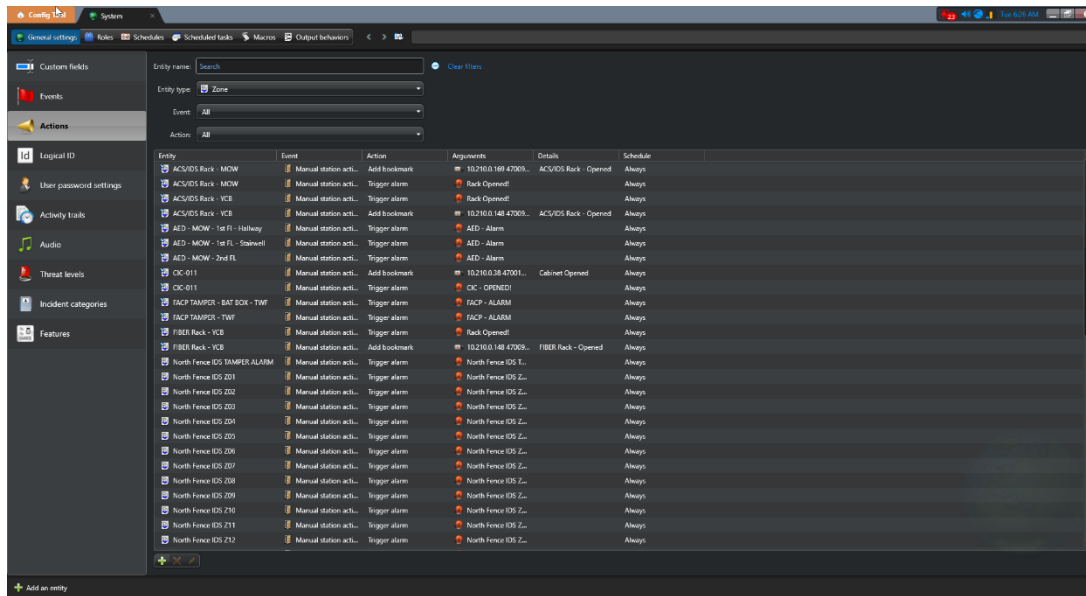


Figure 151. Access Control Configuration: General Settings: Zones

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 240 of 430

There are 3 types of zones:



A Hardware Zone is a collection of one or more inputs on an access control type unit and is managed by the access control hardware.

A Virtual Zone is a collection of one or more inputs on any type unit (including cameras, encoders and access controller) and is SCL's allow by Zone Manager.

An I/O Zone is a collection of inputs on multiple SCL's. Peer to peer communication between the managed inputs states to be linked to output behaviors.

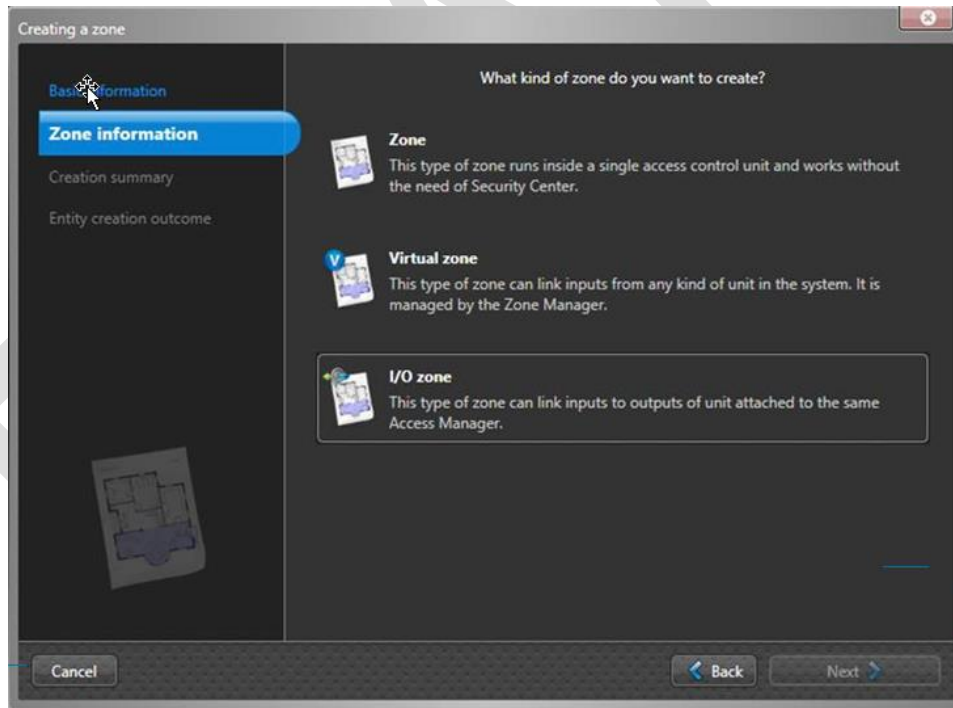


Figure 152. Access Control Configuration: Creating a Zone

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 241 of 430	

3.11.4.1 About Zones

A zone is a type of entity that monitors a set of inputs and triggers events based on their combined states. These events can be used to control output relays.

The concept of a zone is borrowed from the world of alarm panels, where electric inputs are associated with zones to trigger specific alarms. In Security Center, electrical inputs are associated with zones to trigger events. Using event-to-actions, these events can be used to not only trigger outputs, but also to trigger alarms, send emails, start camera recordings, and so on.

TIP: You can also define custom events to correspond to each of the special input combinations.

A zone can be armed (triggers activated), or disarmed (triggers deactivated) using a key switch, a software command, or on a schedule. A zone can be armed by software (using an action command or according to a schedule), or by hardware (for units that support this feature).

3.11.4.2 I/O Linking

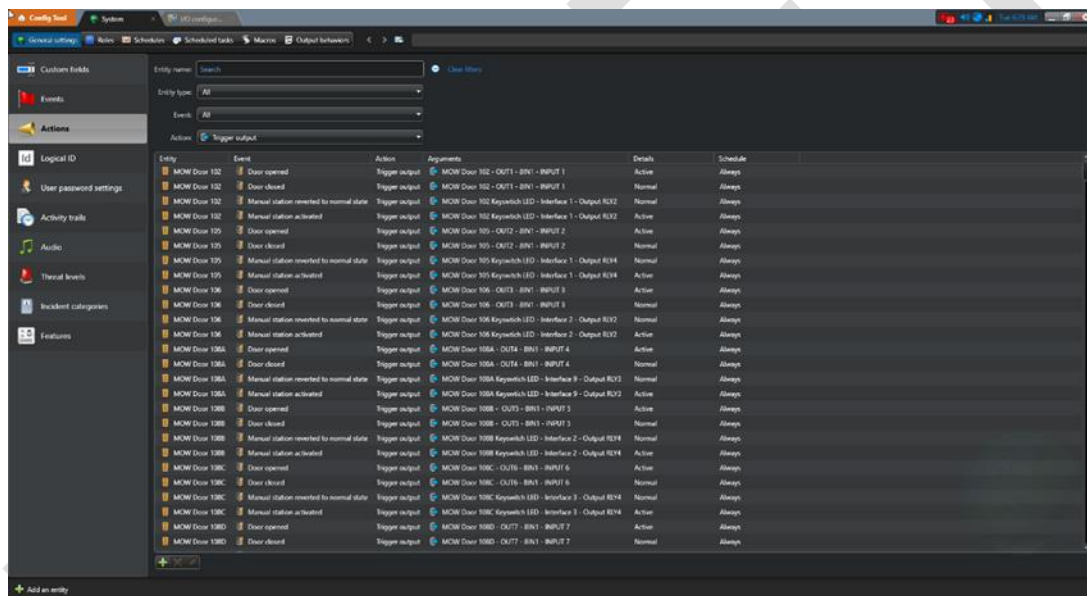


Figure 153. Access Control Configuration: General Settings: In/Out Linking

I/O linking is the control of specific output relays based on the combined result of a specific set of electric inputs. Each input can be connected to a specific monitoring device, such as a motion sensor, a smoke detector, a door or window contact, and so on.

For example, if a window shatters, the glass break sensor on a window connected to an input on a unit, can be linked to an output that triggers a buzzer.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 242 of 430

CAUTION: On HID VertX units, some inputs, such as AC Fail and Bat Fail, must be configured for something other than their initial purpose (leave the checkboxes empty) before they can be used for I/O linking.

However, other inputs, such as Door Monitor, can only be used for their designated purpose. If you use a specific purpose input as general purpose, your configuration will not work. Do not exceed 20 inputs per zone with HID VertX units. Exceeding this limit may lead to unit synchronization problems.

Zone states

Zone states are determined by a combination (**AND/OR**) of inputs associated with the zone. The following zone states are available:

Normal: When the combination of inputs yields a zero (0).

Active: When the combination of inputs yields a one (1).

Trouble: Requires to have at least one supervised input. The zone is in the **Trouble** state when at least one of the input is in the **Trouble** state. The **Trouble** state supersedes all other states.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 243 of 430	

3.11.4.3 Hardware Zones

A hardware zone is a zone entity in which the I/O linking is executed by a single access control unit. A hardware zone works independently of the Access Manager, and consequently, cannot be armed or disarmed from Security Desk.

Hardware zones are recommended when quick responses and offline operations are crucial for your security system. The access control unit controlling the zone must not be operated in server mode. Once the unit is configured in Security Center, it must be able to act on its own without being connected to, or controlled by Security Center.

Hardware zones can be armed using a key switch (input), or on schedules.

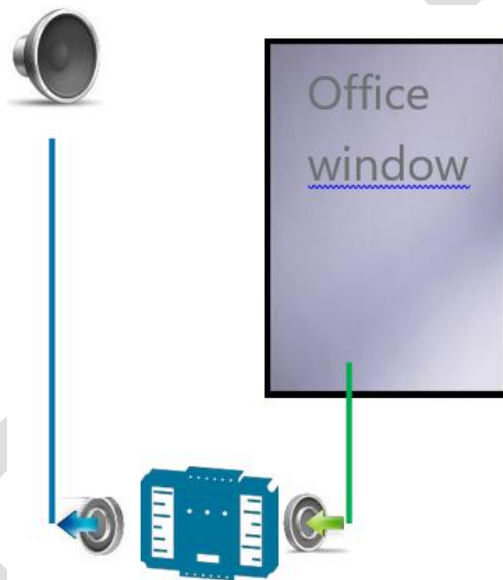


Figure 154. Access Control Unit

Inputs from access control units can trigger custom events.

Ex: Glass Break, IR Motion detection, Smoke detected, Button Pressed.

To monitor a zone, the inputs must be added to Zones.

Hardware Zones handle I/O linking at the access-control unit-level.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 244 of 430

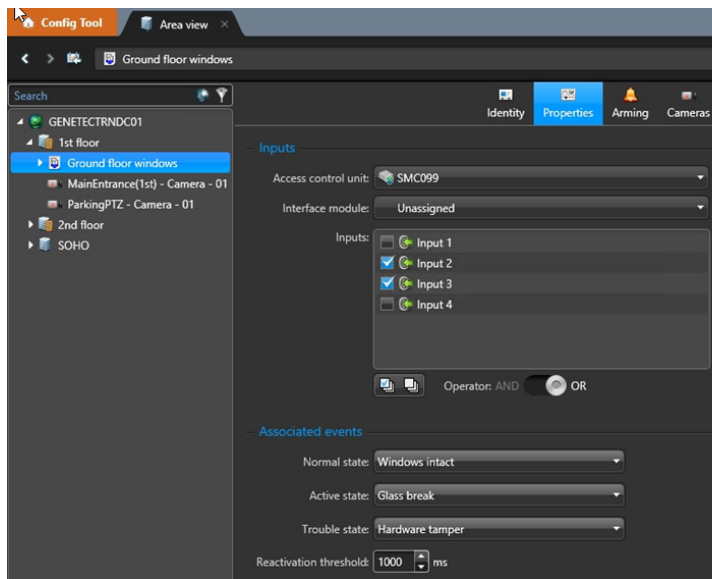


Figure 155. Add Inputs to Zone

Select unit

Add input(s) to
the zone from 1
or more unitsAND = All inputs
must change
stateOR = only 1
input must
change state

Associate events

3.11.4.4 Virtual Zones

A virtual zone is a zone entity where the I/O linking is done by software. The input and output devices can belong to different units of different types. A virtual zone is controlled by the Zone Manager and only works when all the units are online. It can be armed and disarmed from Security Desk.

Virtual zones are recommended when flexibility is required, and when access control units are not available.

3.11.4.5 I/O Zones

An I/O zone is a zone entity in which the I/O linking can be spread across multiple Synergis™ units, while one unit acts as the master unit. All Synergis™ units involved in an I/O zone must be managed by the same Access Manager. The I/O zone works independently of the Access Manager, but ceases to function if the master unit is down. An I/O zone can be armed and disarmed from Security Desk as long as the master unit is online.

I/O zones are recommended when quick responses, offline operation, and I/O linking across multiple units are required.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 245 of 430

3.11.4.6 I/O Linking Example

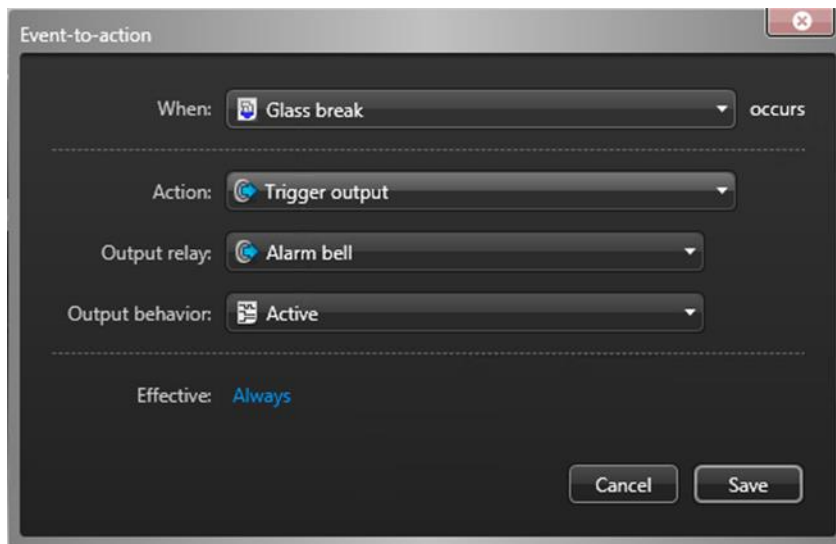


Figure 156. I/O Linking Example

3.11.4.7 Global I/O: Peer-to-Peer Communication on SCL

Enables linking of inputs and outputs between multiple Synergis Cloud Link devices. Inputs activated on multiple devices can trigger outputs on other devices. No server communication required, everything is done within the SCL devices.

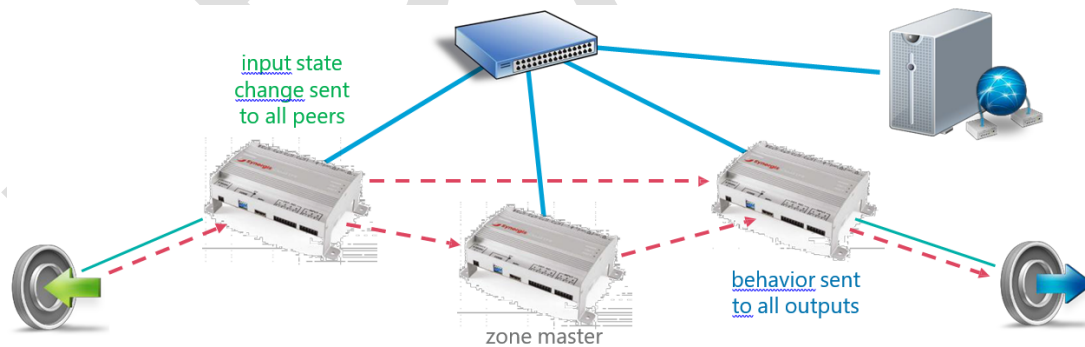


Figure 157. Global I/O: Peer-to-Peer Communication on SCL

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 246 of 430

3.11.4.8 Peer to Peer SCL Communications

Specifications:

All peers must be Synergis Cloud Link (SCL) or Synergis Master Controller (SMC) devices.

All devices must be running *Softwire* version 10.2.

Security Center 5.5 required for configuration.

Uses a new type of zone to establish peers: **I/O zone**.

All peers must be enrolled under the same **Access Manager**.

Can support 15 units, 128 inputs, and 512 outputs.

3.11.4.9 Global I/O; Peer to Peer Setup

Configuration:

If the children of the **Access Manager** need peer-to-peer communication, we need to enable it in the properties of the **Access Manager** first.

Can still use an **I/O zone** for inputs and outputs on the same *SCL/SMC*, but do not need to enable peer-to-peer on the **Access Manager** in this case.

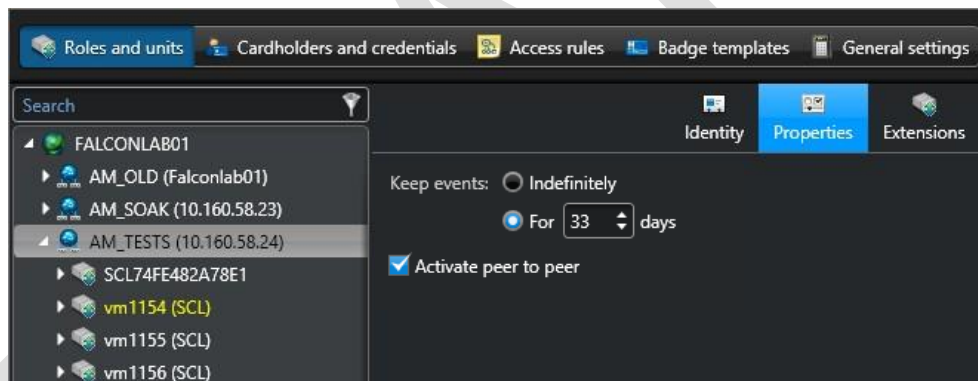


Figure 158. Global I/O; Peer to Peer Setup

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 247 of 430

3.11.4.10 Global I/O; Peer to Peer Configuration

Configuration:

Create a zone as usual.

Choose the new I/O zone.

Select the zone master, which controls all communication with the peers.

Select the arming schedule.

Select the inputs used, outputs to trigger, and the behavior to use.

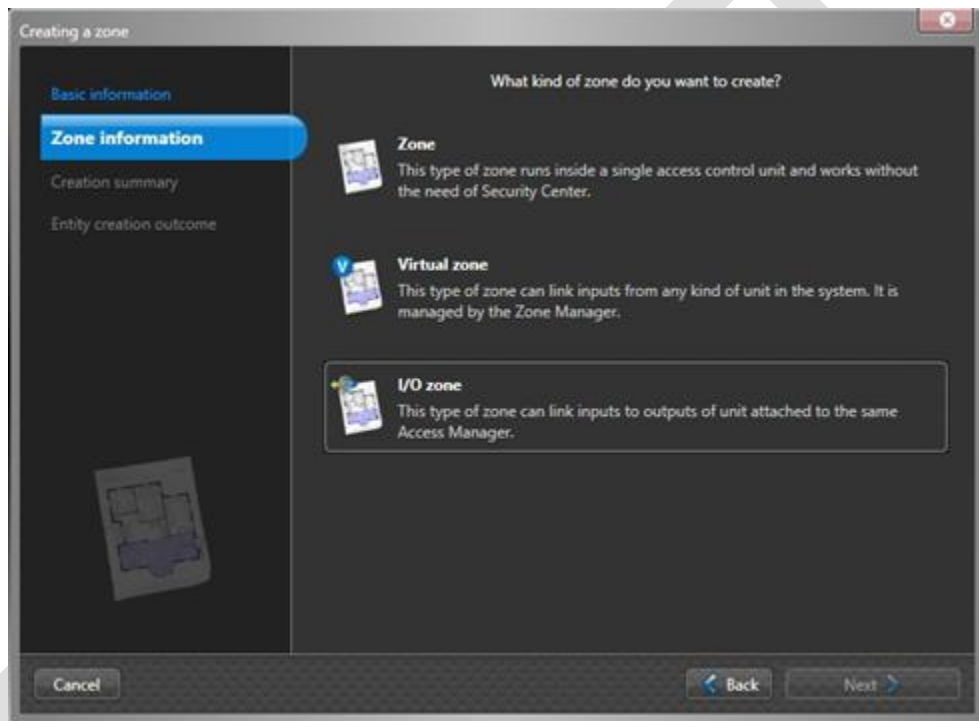


Figure 159. Global I/O; Peer to Peer Configuration

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 248 of 430

3.11.4.11 I/O Zone Properties

State is a logical **OR** with all I/O zone inputs

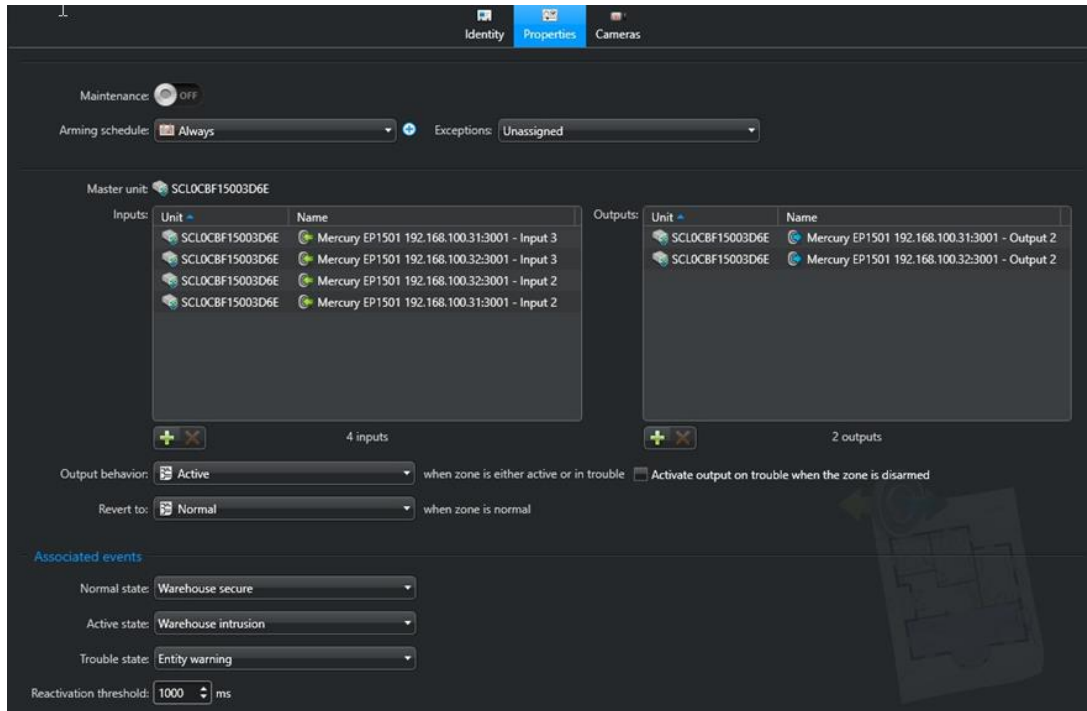


Figure 160. I/O Zone Properties

3.11.4.12 I/O Zone Limitations

Limitations:

- Peer-to-peer communication will not function if the zone master SCL is down.
- No backup zone master available at the moment.
- Access Manager cannot act as the zone master.
- Don't enable peer-to-peer on an Access Manager if not needed (for security and performance).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 249 of 430

3.11.4.13 Differences between the Types of Zone

The following table lists the differences between a hardware zone, a virtual zone, and an I/O zone, and can help you decide which type of zone you need to create.

Table 36. Types of Zones

Characteristics	Hardware zone	Virtual zone	I/O zone
Recommended use	Hardware zones are recommended when quick responses and offline operations are crucial for your security system.	Virtual zones are recommended when flexibility is required, and when access control units are not available.	I/O zones are recommended when quick responses, offline operation, and I/O linking across multiple units are required.
Role	Access Manager	Zone Manager	Access Manager
Required unit type	HID or Synergis™ unit	Any type of unit with inputs and outputs ¹	Synergis™ units ²
Unit operation mode	Online and Offline	Online	Online and Offline
I/O linking execution	Access control unit	Zone Manager	Master unit ³
I/O linking (inputs)	All inputs must be from the same unit	Can combine inputs from any unit of any type	Can combine inputs from any unit
Logical operator (inputs)	OR/AND	OR/AND	OR
I/O linking (outputs)	All outputs must be from the same unit as the inputs	Can trigger outputs on any unit of any type	Can trigger outputs on any unit
I/O linking configuration	Zone configuration + event-to-actions	Zone configuration + event-to-actions	Zone configuration alone
Peer-to-peer	No	No	Yes ⁴
Arm/disarm from Security Desk	No	Yes	Yes ⁵
Arm/disarm using actions	No	Yes	Yes ⁵
Arm/disarm using key switch	Yes ⁶	No	No
Arm/disarm on schedule	Yes ⁷	Yes ⁸	Yes ⁹
Arming delay	OFF/ON (mm:ss)	OFF/ON (mm:ss)	No
Entry delay	OFF/ON (mm:ss)	OFF/ON (mm:ss)	No
Maintenance mode	No	No	Yes

¹ Using zones to monitor the inputs of intrusion detection units is not recommended.

² Requires Security Center 5.5 and later, and Synergis™ Softwire 10.2 and later.

³ The master unit is the Synergis™ unit that you select to do I/O linking.

⁴ Up to 15 Synergis™ units can communicate directly with each other, as long as they are all under the same Access Manager.

⁵ The master unit must be online.

⁶ The key switch must be wired to an input on the same access control unit.

⁷ Only one schedule at a time, and cannot be combined with the key switch approach.

⁸ Supports multiple schedules.

⁹ Supports multiple schedules, including exception schedules.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 250 of 430

3.11.4.14 About Zone Managers

Zone Manager is a type of role that manages virtual zones and triggers events or output relays based on the inputs configured for each zone. It also logs the zone events in a database for zone activity reports.

Multiple instances of this role can be created on the system.

3.11.4.15 About Output Behaviors

An output behavior is a type of entity that defines a custom output signal format, such as a pulse with a delay and duration.

Some examples of output behaviors can include controlling a parking gate, flashing a light in the warehouse, and so on.

Output behaviors are used to control output relays or access control units, video units, and zones that are not being used to control door locks. They can be triggered by automatic event-to-actions, manually through hot actions in Security Desk, or through I/O linking.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 251 of 430	

3.11.4.16 Creating Hardware Zones

To have a zone that can operate on its own even when the access control unit is not connected to the Access Manager, you must create a hardware zone in Security Center.

Do the following:

Configure the **Access Manager** role that will manage the zone.

Add the access control unit that will control the zone in your system.

A hardware zone allows you to program the I/O linking behavior on an access control unit so it can operate on its own. Hardware zones can only be controlled by a single access control unit.

To create a hardware zone:

1. Open the Area view task.
2. Click **Add an entity** (+) > **Zone**.
3. In the **zone creation** wizard, enter a name and description for the zone.
4. Select the area this zone is part of in **Location**, and click **Next**.
5. On the **Zone information** page, click **Hardware zone**.
6. From the dialog box, select the access control unit to control this zone and click **OK**.
7. Click **Create** > **Close**.

After you finish

Configure the hardware zone

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 252 of 430

3.11.4.17 Configuring Hardware Zone Settings

To monitor and set up I/O linking for hardware zones in Security Center, you must decide how the zone state is evaluated, which events are triggered based on the inputs associated with the zone, and when the zone is armed.

Do the following:

To arm the zone on a schedule, a schedule must already be created.

To arm the zone using a key switch, one of the inputs from the access control unit must be wired to the key switch.

All input points and output relays configured for this zone must belong to the same access control unit that is controlling the zone.

You cannot arm or disarm a hardware zone from *Security Desk*, or by using a software command (event-to- actions).

To configure hardware zone settings:

1. Open the **Area view** task.
2. Select the hardware zone to configure, and click the **Properties** tab.
3. From the list, select the inputs to determine the state of the zone.
4. Turn the **Operator switch** to the desired position.
 - **AND:** Combine the input states with the logical **AND** operator.
 - **OR:** (Default) Combine the input states with the logical **OR** operator

Example: If you select the **AND** operator, the zone is considered to be in an **Active** state when all selected inputs are in the **Active** state. If you select the **OR** operator, the zone is considered to be in an **Active** state if one of the selected inputs is in the **Active** state.

5. In the **Associated events** section, select which events to trigger when the zone state changes, from the following drop-down lists:

These events are only triggered when the zone is armed. Select **None** if a zone state should be ignored.

- **Normal:** When the combination of inputs yields a zero (0).
 - **Active:** When the combination of inputs yields a one (1).
 - **Trouble:** Requires to have at least one supervised input. The zone is in the **Trouble** state when at least one of the input is in the **Trouble** state. The **Trouble** state supersedes all other states.
6. Enter in **Reactivation threshold**, how many milliseconds must pass before the event associated to the zone state can be re-triggered, and click **Apply**.
 7. Click the **Arming** tab, and configure how the zone is armed.
 8. In the **Arming source** section, select whether the zone is armed using a key switch, or on a schedule:
 - **Schedule:** Select a predefined schedule for arming the zone.
 - **Input point:** Select the input that is wired to the key switch.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 253 of 430

9. (Optional) To give people more time to leave a zone they just armed, or disarm a zone they entered, turn the following options **ON**:
- **Arming delay**: Duration (mm:ss) you want between the time the zone is armed and the time the event triggers become active.
 - **Entry delay**: Duration (mm:ss) you want between the time the entry sensor is tripped and the time the events are triggered. This option allows you to disarm the zone before triggering the output relays.
10. 1(Optional) Select a **Countdown** buzzer to use for the duration of the arming delay, as follows:
- NOTE**: This option is only available when the zone is armed using a key switch.
- From the **Countdown sounder** drop-down list, select an output relay.
 - From the **Output behavior** drop-down list, select an output behavior entity to determine the pattern of the signal to send to the buzzer.
11. Click **Apply**.

After you finish

- Test your zone by verifying that the generated events show up in the **Zone activities** report in *Security Desk*. For more information, see the *Security Desk User Guide*.
- For each associated event configured for this zone, create *event-to-actions* to trigger the desired output relays to complete the I/O linking configuration.

NOTE: For the hardware zone to work, the output relays must be among the peripherals of the unit controlling the zone.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 254 of 430

3.11.4.18 Creating Virtual Zones

To monitor input devices (sensors, switches, and so on) using *Security Desk*, and to use them to trigger events, you must create a virtual zone in *Security Center*.

Configure the **Zone Manager** role that will manage the zone.

A virtual zone allows you to turn monitoring on/off in the various input devices (sensors, switches, and so on) on your system using *Security Desk*, and to use them to trigger events.

To create a virtual zone:

1. Open the **Area view** task.
2. Click **Add an entity** (+) > **Zone**.
3. In the **zone creation** wizard, enter a name and description for the zone.
4. Select the area this zone is part of in **Location**, and click **Next**.
5. In the **Zone information** page, click **Virtual zone**.

If you have multiple **Zone Manager** roles, you are prompted to select one.

6. Click **Create** > **Close**.

After you finish

Configure the virtual zone.

3.11.4.19 Configuring Virtual Zone Settings

To monitor input devices and use them to trigger events for virtual zones in *Security Center*, you must decide how the zone state is evaluated, which events are triggered based on the inputs associated with the zone, and when the zone is armed.

To arm the zone on a schedule, a schedule must already be created.

A virtual zone can be armed at any time by a *Security Desk* operator, or by the **Arm zone** action.

Arming schedules is optional and is only necessary if you want the zone to be armed automatically at a certain time. An armed virtual zone can be disarmed at any time by a *Security Desk* user, or by the **Disarm zone** action triggered by an event.

To configure virtual zone settings:

1. Open the **Area view** task.
2. Select the virtual zone to configure, and click the **Properties** tab.
3. Under the **Inputs** list, click **Add an item** (+), select the inputs that will determine the state of the zone, and click **Select**.

TIP: Hold **Ctrl** or **Shift** to select multiple inputs.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 255 of 430

4. Turn the **Operator** switch to the desired position.
 - **AND**: Combine the input states with the logical **AND** operator.
 - **OR**: (Default) Combine the input states with the logical **OR** operator

Example: If you select the **AND** operator, the zone is considered to be in an **Active** state when all selected inputs are in the **Active** state. If you select the **OR** operator, the zone is considered to be in an **Active** state if one of the selected inputs is in the **Active** state.
5. In the **Associated events** section, select which events to trigger when the zone state changes, from the following drop-down lists:

These events are only triggered when the zone is armed. Select **None** if a zone state should be ignored.

 - **Normal**: When the combination of inputs yields a zero (0).
 - **Active**: When the combination of inputs yields a one (1).
 - **Trouble**: Requires to have at least one supervised input. The zone is in the Trouble state when at least one of the input is in the Trouble state. The Trouble state supersedes all other states.
6. Enter in **Reactivation** threshold, how many milliseconds must pass before the event associated to the zone state can be re-triggered, and click **Apply**.
7. Click the **Arming** tab, and configure how the zone is armed.
8. Under the **Arming source** section, click **Add an item** (+), select a predefined schedule for when the zone is armed, and click **Select**.
9. (Optional) To give people more time to leave a zone they just armed, or disarm a zone they entered, turn the following options **ON**:
 - **Arming delay**: Duration (mm:ss) you want between the time the zone is armed and the time the event triggers become active.
 - **Entry delay**: Duration (mm:ss) you want between the time the entry sensor is tripped and the time the events are triggered. This option allows you to disarm the zone before triggering the output relays.
10. Click **Apply**.

After you finish

- Test your zone by verifying that the generated events show up in the **Zone activities** report in *Security Desk*. For more information, see the *Security Desk User Guide*.
- For each associated event configured for this zone, create event-to-actions to trigger the desired output relays to complete the **I/O linking** configuration.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 256 of 430

3.11.4.20 Creating I/O Zones

To have the inputs on one Synergis™ unit trigger output relays on other Synergis™ units (even when some, or none of them are connected to the Access Manager), you must create an I/O zone in *Security Center*.

Do the following:

Configure the **Access Manager** role that will manage the zone.

Add the Synergis™ units that will be linked by the zone.

Make sure all units are running Synergis™ Software version 10.2 or later.

An I/O zone allows you to program the I/O linking behavior on multiple Synergis™ units, with one unit designated as the master unit. All units must be managed by the same **Access Manager**. An I/O zone can be armed and disarmed from *Security Desk* as long as the master unit is online.

To create a hardware zone:

1. Open the **Area view** task.
2. Click **Add an entity** (+) > **Zone**.
3. In the **zone creation** wizard, enter a name and description for the zone.
4. Select the area this zone is part of in **Location**, and click **Next**.
5. In the **Zone information** page, click **I/O zone**.
6. From the dialog box, select the **Synergis™** unit that will play the role of master unit among its peers, and click **OK**.

The master unit is the Synergis™ unit that you select to do I/O linking. Once your choice is made, it cannot be changed after the **I/O zone** is created.

7. Click **Create** > **Close**.

After you finish

Configure the I/O zone.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 257 of 430

3.11.4.21 Configuring I/O Zone Settings

To monitor and set up I/O linking for I/O zones in *Security Center*, you must decide how the zone state is evaluated, which output relays are triggered based on the inputs associated with the zone, and when the zone is armed.

Do the following:

To arm the zone on a schedule, a schedule must already be created.

To trigger an output relay, an output behavior must already be created.

All input points and output relays configured for this zone must belong to Synergis™ units that are managed by the same **Access Manager**.

You can configure the I/O linking from the I/O zone's Properties tab. You do not need to create event-to- actions in order to trigger output relays.

IMPORTANT: If the inputs and outputs configured for this zone do not belong to the same Synergis™ unit, you must enable the Activate peer to peer option on the Access Manager.

To configure I/O zone settings:

1. Open the **Area view** task.
2. Select the I/O zone to configure, and click the **Properties** tab.
3. From the **Arming schedule** drop-down list, select a predefined schedule for when the zone is armed.

To add more predefined schedules for defining the arming schedule, click **Advanced** (+) and then click **Add an item** (+).
4. (Optional) Click **Exceptions** to define periods within the arming schedule when the zone should not be armed.
5. Under the **Inputs** list, click **Add an item** (+), and select inputs to determine the state of the zone. The zone is considered to be in a **Trouble** state if one of the inputs is in the **Trouble** state.
6. Under the **Outputs** list, click **Add an item** (+), and select the output relays that you want to send the configured output behavior to, when the zone is armed and in the **Active** state, or when the zone is in the **Trouble** state.

BEST PRACTICE: As much as possible, use the output relays on the master unit. This allows the I/O zone to continue to function when one or more slave units are down.
7. From the **Output behavior** drop-down list, select the output behavior to send to the output relays.
8. Select **Activate output on trouble** when the zone is disarmed if you want the output relays to be triggered when the zone is in the **Trouble** state.
9. From the **Revert to** drop-down list, select the output behavior to send to the output relays when the zone returns to the **Normal** state.
10. In the **Associated events** section, select which events to trigger when the zone state changes, from the following drop-down lists:

These events are only triggered when the zone is armed. Select **None** if a zone state should be ignored.

- • **Normal:** When the combination of inputs yields a zero (0).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 258 of 430

- **Active:** When the combination of inputs yields a one (1).
- **Trouble:** Requires to have at least one supervised input. The zone is in the **Trouble** state when at least one of the input is in the **Trouble** state. The **Trouble** state supersedes all other states.

11. Enter in **Reactivation threshold**, how many milliseconds must pass before the event associated to the zone state can be re-triggered, and click **Apply**.

After you finish

Test your zone by verifying that the generated events show up in the **Zone** activities report in *Security Desk*. For more information, see the *Security Desk User Guide*.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 259 of 430

3.11.5 Advanced Access Control

This section includes:

[“Import Cardholders from Active Directory”](#)

[“How AD Integration Works”](#)

To import users and/or cardholders from an AD, you must create an **Active Directory** role for the AD you want to import. The **Active Directory** role connects your *Security Center* system to an Active Directory server, and imports users and/or cardholders from selected security groups. Imported entities are identified in *Security Center* by a yellow arrow (👉) superimposed on the regular entity icon.

The **Active Directory** role synchronizes all the changes made on the AD with the imported entities in *Security Center*. It also pushes the logon credentials of imported users to the AD service for validation.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 260 of 430

3.11.5.1 Benefits of AD Integration

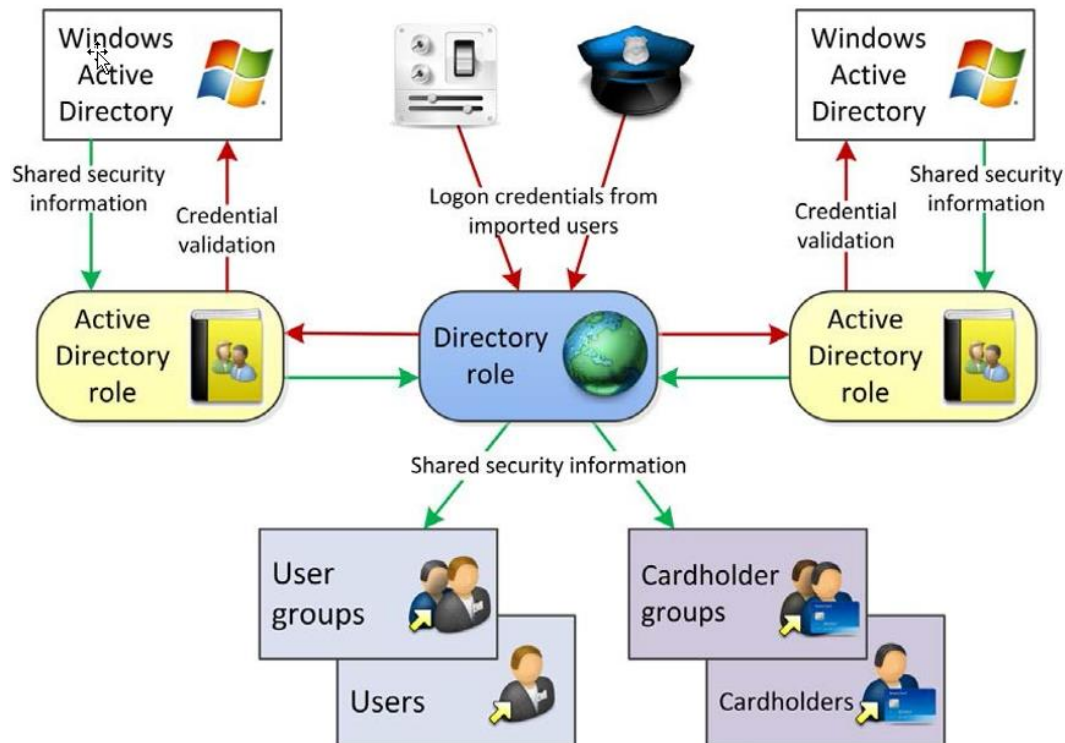


Figure 162. Benefits of Active Directory Integration

Having a centralized security information management system provides many benefits:

Less data entry means fewer errors and better control during initial *Security Center* setup, because users and cardholders can be imported from an existing AD.

Consistency and better security because all shared information is entered only once.

- A new user account that is added to an imported security group automatically adds a new user and/or cardholder in *Security Center*.
- A user account that is disabled in the AD automatically disables the corresponding user and/or cardholder in *Security Center*.

Single logon capability for synchronized *Security Center* users. Users logged on to Windows do not have to log on to *Security Center*.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 261 of 430

3.11.5.2 Active Directory Synchronization

Through a process called synchronization, the **Active Directory** role also keeps all imported entities up-to-date with changes made on the AD.

All imported entities are synchronized with their source by the **Active Directory** role. Most of the attributes imported from the AD are read-only in *Security Center*, except for a few cardholder properties. Imported entities cannot be deleted unless they are deleted from the AD.

CAUTION: If you move a security account from a synchronized AD security group to one that is not synchronized, it is as though the account ceases to exist in *Security Center*. The Active Directory role deletes the corresponding entities (users and/or cardholders) from *Security Center* the next time it synchronizes with the AD.

Synchronization is always initiated from *Security Center*. There are two ways that you can start synchronization:

- **Manually:** Synchronization is performed when you explicitly request it. This is the default setting. The advantage of this approach is that you have perfect control over when you want the synchronization to be done.

- **On schedule:** The imported groups are synchronized using a scheduled task.

Information that can be synchronized with the AD

Both standard and custom *Security Center* fields can be imported from the AD, and kept synchronized with the AD. You can choose which user group, user, cardholder group, and cardholder fields to import from the AD in the Links tab of the **Active Directory** role.

The standard attributes you can import from the AD are:

User group

- Name
- Description
- Email address
- All group members (users)

User

- Membership in the imported user group
- Username
- Password
- Description
- First name
- Last name
- Email address
- Status: Active or Inactive

• Cardholder group

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 262 of 430

- Name
- Description
- Email address
- All group members (cardholders)
- **Cardholder**
 - Membership in the imported cardholder group
 - Cardholder name
 - Description
 - First name
 - Last name
 - Email address
 - Status: Active or Inactive
 - Picture (optional through the Links tab)
 - Partition (optional through the Links tab)

Credential

- Association to the imported cardholder
- Credential name
- Card data
- Card format
- Facility code
- Card number
- Status: Active or Inactive
- Partition (optional through the Links tab)

Additional attributes are imported from the AD by mapping them to *Security Center* custom fields. The **Active Directory** role keeps all imported fields synchronized with the AD.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 263 of 430

3.11.5.3 About Universal Groups and Global Catalogs

Security Center supports synchronizing Universal groups that belong to a global catalog. Users from different domains in an AD forest can access *Security Center* using one **Active Directory** role connected to one domain controller (global catalog). There are some things you should know before synchronizing a Universal group that belongs to a global catalog.

Note the following when importing a Universal group that belongs to a global catalog:

There must be a trust relationship configured between all domains in the AD forest.

Primary groups are not supported.

In order to retrieve the directories within a forest, the Active Directory role user must be able to read the *CN=Partitions*, *CN=Configuration*, *DC=ROOTDOMAIN*, *DC=COM* folder.

If you are importing a Universal group that does not belong to a global catalog:

- The **Active Directory** role contacts several ADs. The **Active Directory** role user must have the necessary permissions to access the different ADs within a forest.
- The default port used to contact the AD is 389. If you are using a different port, you must append it to the AD server name defined in the **Active Directory** field on the **Properties** tab, for example: **ADServer.Genetec.com:3393**.

If you are importing a Universal group that belongs to a global catalog:

- The global catalog must be updated to include the attributes required for *Security Center* user and cardholder information. For the list of required attributes, see [Global Catalog Attributes](#).
- The default port used to contact the AD is 3268. If you are using a different port, you must append it to the AD server name defined in the **Active Directory** field on the **Properties** tab. The name and port number must be separated by a colon, for example:
ADServer.Genetec.com:3295.

Benefits of using a global catalog

A global catalog stores a copy of all AD objects in a forest which provides many benefits:

The need to query multiple domains for information is eliminated since everything is stored in the global catalog.

Less time to process information.

Less bandwidth used.

Less replication of information.

Requires only a single **Active Directory** role connection. All users can access *Security Center* using the global catalog.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 264 of 430

3.11.5.4 Importing Security Groups from an Active Directory

To have a centralized personnel management system, you can import AD security groups into Security Center as user groups or cardholder groups.

If you are importing a universal group from a global catalog, read About universal groups and global catalogs.

When importing an AD security group, you must import all members of that group, including the subgroups. If you want to import only a subset of its members, for example, only *Security Center* users, you must define a new AD security group with only the members you want to import.

If you are integrating multiple ADs into *Security Center*, they must each belong to a different domain.

If you have servers in your system that are running an earlier version of *Security Center*, you must upgrade the servers to the current version before using them to host a new **Active Directory** role.

- An AD security group can be imported as user group, cardholder group, or both.

To import a security group:

1. Open the **System** task, and click the **Roles** view.
2. Click **Add an entity** (+) and select **Active Directory**.
3. On the **Specific info** page, do the following:
 - A. (If you have multiple servers in your system) From the **Server** drop-down list, select the server on which you want to host the role.
 - B. In the **Active Directory** field, enter the AD Fully Qualified Domain Name (FQDN), hostname, or IP address of the AD server.

If you are not using a default port, you must append the port number you are using to the AD server name, separated by a colon. For example, **ADServer.Genetec.com:123**. The default ports are as follows:

- Active Directory with no SSL: 389
 - Active Directory with SSL: 636
 - Global catalog no SSL: 3268
 - Global catalog with SSL: 3269
- C. Specify how you want the role to connect to the AD server. You must have read access to the selected AD service.
 - Use the Windows credentials assigned to the *Genetec™ Server* service that is running on the server hosting the **Active Directory** role.
 - Specify a different set of Windows credentials (username, password).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 265 of 430

4. On the **Basic information** page, enter the name, description, and partition where you want to create the **Active Directory** role.
5. Click **Next**, **Create**, and **Close**.

A new **Active Directory** role () is created. Wait a few seconds for the role to connect to the AD server.

6. (Optional) If you are importing a universal group that connects to a global catalog, turn on the **Use global catalog** option.
7. On the **Properties** tab, select the AD security groups you want to import.

NOTE: There are two types of groups in Windows Active Directory: distribution groups and security groups. Security Center can only synchronize with security groups.

A. Click **Add an item** ().

B. Select the security groups you want to add to your **Active Directory** role. Use one of the following methods:

- (Recommended) Type the name of the group in **Find Active Directory** groups, and click ().

If the text you entered matches a single group, it is automatically added to the **Selected groups** list.

If the text you entered matches multiple group names, a second dialog box appears listing all the group names that match the text you entered.

Select the ones you want, and click **OK** to add them to the **Selected groups** list.

- From the **Selected groups** list, click ().

The **Active Directory members** dialog box appears.

Select a security group, and click **OK**. Only security groups can be synchronized. If you selected an item that is not a security group, the **OK** button remains disabled.

NOTE: The names shown in the dialog box are display names. *Security Center* only synchronizes the account names because they are guaranteed to be unique. Typically, the display names and the account names are the same. The only way to tell them apart is that the display names contain spaces.

- C. Repeat the previous step as often as necessary until all security groups you want to synchronize with the AD are listed in **Selected groups**, and then click **OK**.

The selected groups are listed under **Synchronized groups** in the **Properties** tab.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 266 of 430

8. For each of the synchronized groups, specify how you want to import them.

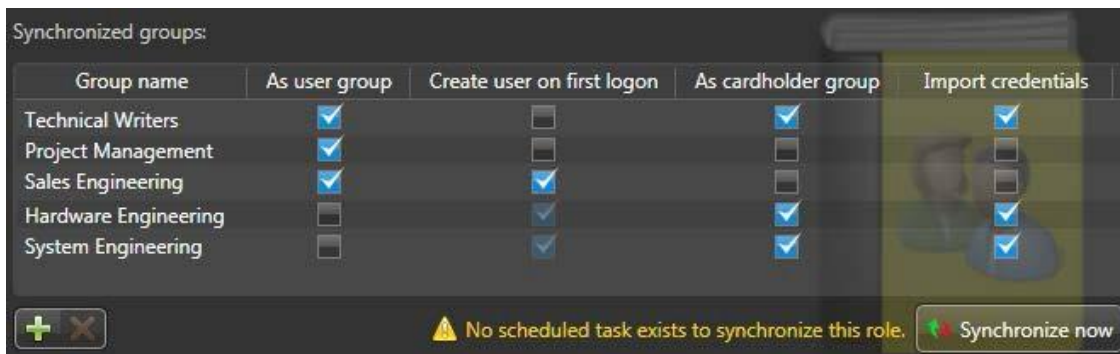


Figure 163. Synchronized Groups

The following options are available:

- **As user group:** Select this option to import the synchronized group as user group, and the group members as users.
 - **Create user on first logon:** This is the default option, and it creates an empty user group. User entities are only created when someone tries to logs on the first time. This option avoids having to create all user entities simultaneously, which can freeze up the system. If you clear this option, all user entities are created at the same time as a user group.
 - **As cardholder group:** Select this option to import the synchronized group as cardholder group, and the group members as cardholders. All synchronized cardholders are created simultaneously.
 - **Import credentials:** Select this option to import the credential information of the synchronized cardholders.
9. If you are importing the AD security group as cardholder group, select which cardholder fields you want to synchronize with the AD.
 10. (Optional) Map custom fields to synchronize with the AD.
 11. Click **Apply**, and then click **Synchronize now** (🔄).

All synchronized groups and their members are imported as *Security Center* entities according to your specifications, with a yellow arrow (👉) superimposed on their icon.

After you finish

Some additional configuration might be required, depending on what you synchronized with the AD:

If you already had entities configured in your system, you might need to resolve certain conflicts due to the import.

(Optional) Configure the imported user groups with proper privileges and security options, so that when new user entities are created, they can automatically inherit these properties from their parent user group.

(Optional) Configure the imported cardholders and cardholder groups.

(Optional) Create a scheduled task to synchronize imported entities with the AD on a regular

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 267 of 430

basis.

After you create a scheduled task, the warning message **No scheduled task exists to synchronize this role** disappears from the **Properties** tab.

DRAFT

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 268 of 430	

3.11.5.5 Mapping Custom Fields to Synchronize with Active Directory

In addition to default attributes, you can import other attributes from the AD by mapping them to *Security Center* custom fields. The custom field mapping can be different for each **Active Directory** role in your system.

Make sure that the workstation where **Config Tool** is running is on the same network domain as the AD server.

Define the custom fields that will receive data from the AD.

No more than 32 custom fields can be mapped to the AD.

To map custom fields to synchronize with Active Directory:

1. From the **Links** tab of the **Active Directory** role, under **Custom fields**, click **Add an item** (+).

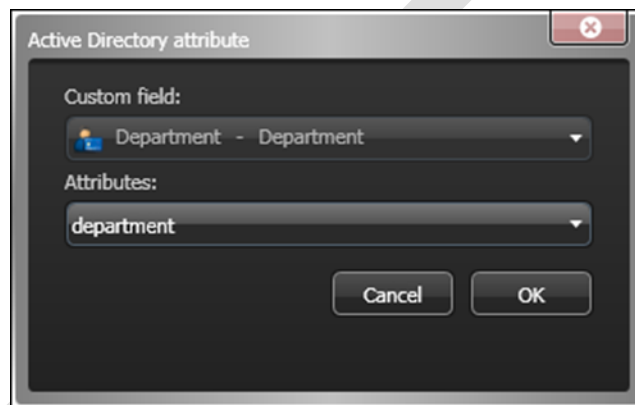


Figure 164. Active Directory Attribute

2. Select the custom field and the AD attribute, and then click **OK**.

IMPORTANT: The data type of the custom field must match that of the AD attribute: text with text, decimal with decimal, date with date, etc. The Security Center image data type must be mapped to the AD binary data type, and the mapped AD attribute must contain a valid JPEG image.

The new mapping appears in the **Links** tab.

3. Repeat the previous steps as needed.
4. Click **Apply**.

The mapped custom fields are displayed in the **Links** tab. When you synchronize with the AD, they are read-only.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 269 of 430

3.11.5.6 Resolving Conflicts Caused by Imported Entities

Conflict resolution might be necessary if you have existing entities (users or cardholders) in your database before importing entities from the AD.

When a synchronized entity has the same name as a local entity, the Active Directory role sees it as a potential conflict. You can use the Conflict resolution tool to view potential conflicts (🔍) and resolve them by deleting the conflicting entities in the the Cardholder Management task.

To resolve conflicts caused by imported entities:

1. Open the **System** task, and click the **Roles** view.
2. Select the Active Directory role (🔍), and click Conflict resolution (🔍).

The **Active Directory conflict resolution** dialog box opens. All synchronized entities are listed to the left. The ones that conflict with a local entity are flagged in green.

3. Resolve each cardholder conflict:
 - A. Open the **Cardholder Management** task and find the two cardholder records that are in conflict.
 - B. Select one of the conflicting cardholder records and click **Modify**.
 - C. Add any missing information that is available in the duplicate cardholder record.
 - D. Save and close the cardholder record.
 - E. Select the duplicate cardholder record and click **Delete Cardholder**.
4. Resolve each user conflict:
 - A. Open the **User Management** task.
 - B. In the entity browser, find the two user records that are in conflict.
 - C. Open one of the conflicting user records.
 - D. Add any missing information that is available in the duplicate user record.
 - E. Click **Apply**.
 - F. Select the duplicate user record and click **Delete**.
5. Return to the **Roles** view in the **System** task.
6. In the **Active Directory conflict resolution** dialog box, select the entities that are flagged as being in conflict and press **Delete**.
7. In the **Active Directory conflict resolution**, click **Finish**.

This process will generate a file named **Conflict_Manifest data** that documents resolved conflicts. It can be saved for future reference.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 270 of 430

3.11.5.7 Deactivating Users Imported from an Active Directory

If you have users that are imported from an Active Directory, you can set the user's status to inactive. The user becomes desynchronized from the AD until you activate the user again.

To deactivate a user imported from an Active Directory:

1. Open the **Security** task.
2. Select an imported user (👤), and click the **Properties** tab.
3. Set the **User status** option to **Inactive**.
4. Click **Apply**.

The user is no longer synchronized with the AD. It will only become synchronized again once you set the user's status to **Active**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 271 of 430

3.11.5.8 Global Catalog Attributes

For the Active Directory role to successfully connect to a global catalog and synchronize users and cardholders in Security Center, the global catalog must be updated to include specific attributes.

User attributes

The global catalog must be updated with the following user attributes:

distinguishedName
objectGUID
objectClass
cn
objectSid
sAMAccountName
displayName
name
mail
description
userPrincipalName
userAccountControl
accountExpires
givenName
sn
tokenGroup
memberof (For the SDK only)
any attributes to be used in the **Links** tab

Group attributes

The global catalog must be updated with the following group attributes:

distinguishedName
objectGUID
objectClass
cn
objectSid
sAMAccountName
name
mail

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 272 of 430

description

groupType

member

Container, domain, and organizational unit attributes

The global catalog must be updated with the following container, domain, and organizational attributes:

distinguishedName

objectGUID

objectClass

objectSid

displayName

name

member

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 273 of 430

Areas: Antipassback and Interlocking”

“Enabling Global Antipassback on Access Manager Roles

If the areas on which you want to apply the antipassback restrictions are controlled by multiple *Synergis*™ units, you must enable global antipassback on the **Access Manager** roles.

When strict and hard antipassback is applied to an area without global antipassback, a cardholder who entered the area through one door cannot leave the area through another door if both doors are not controlled by the same unit. Also, the same cardholder who entered the area through one door, can re- enter the area through a different door if the two doors are not controlled by the same unit. With global antipassback enabled, these two violations can be prevented.

IMPORTANT: Global antipassback only works on areas that are entirely controlled by *Synergis*™ units. All units controlling the same area must be managed by the same Access Manager.

TIP: If you need to switch your units between **Access Manager** roles to meet the global antipassback requirements, use the [Move Unit Tool](#).

To enable global antipassback on an Access Manager role:

1. From the **Config Tool** home page, open the **Access control** task, and click the **Roles and units** view.
2. Select the **Access Manager** role to configure, and click the **Properties** tab.
3. On the **Properties** page, select the following options: **Enable peer to peer** and **Enable global antipassback**.

NOTE: Up to 15 *Synergis*™ units can be connected as peers.

4. Click **Apply**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 274 of 430

3.11.5.9 Areas: Interlock

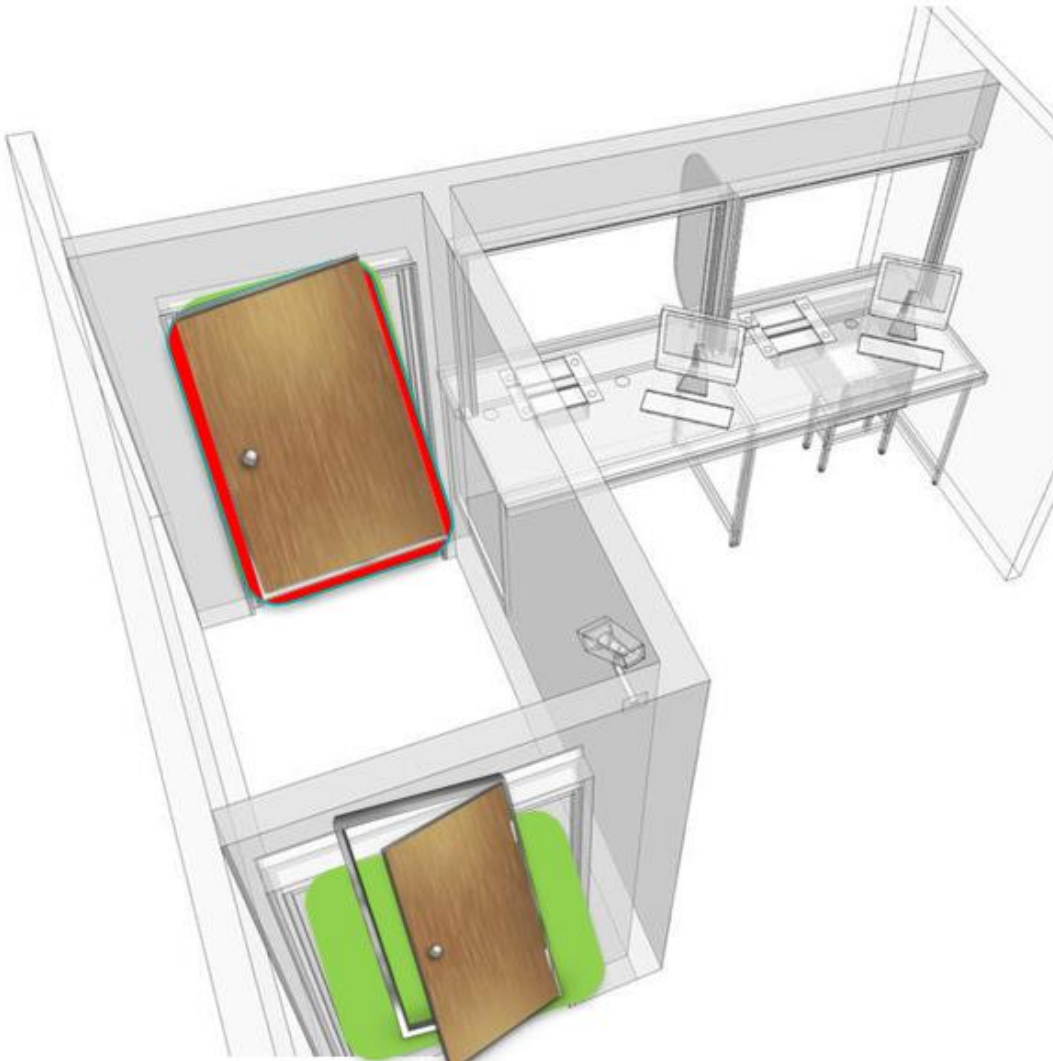


Figure 166. Interlock: Access Granted to 1 Door at a Time

Access is granted one door at a time while access to the interior cannot be accessed without appropriate credentials.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 275 of 430

3.11.5.10 Areas: Interlock Override

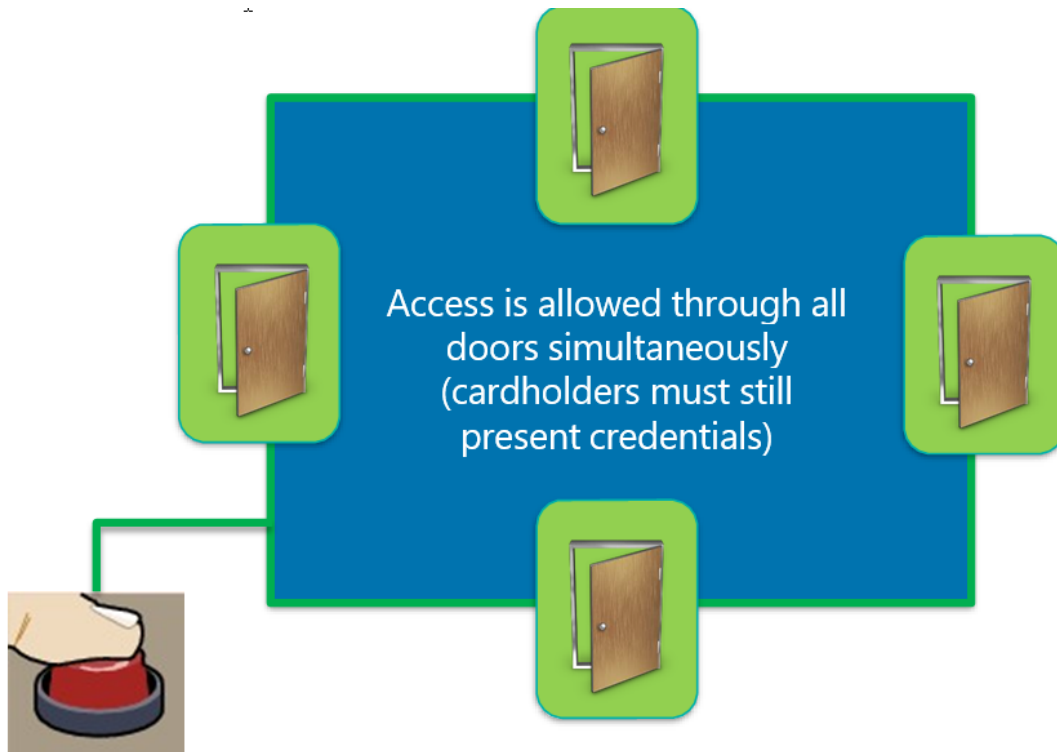


Figure 167. Interlock: Interlock Override

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 276 of 430	

3.11.5.11 Areas: Interlock Lockdown

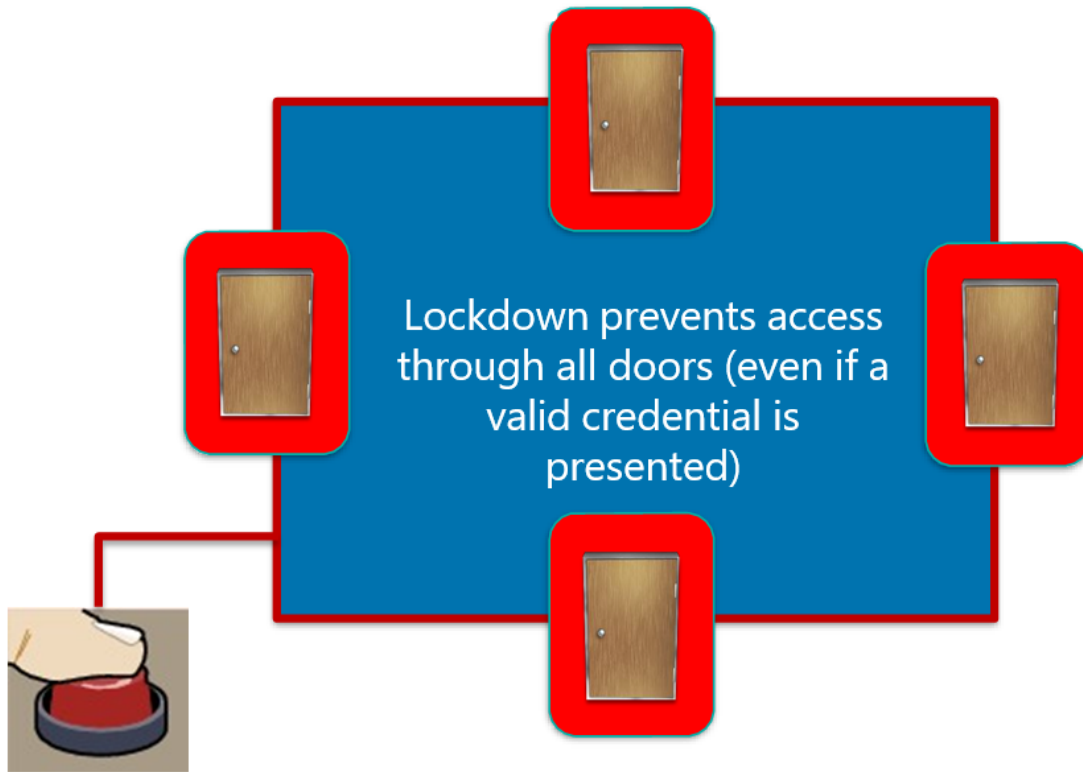


Figure 168. Interlock: Lockdown

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 277 of 430	

3.11.5.12 Interlocking Doors within Areas

Once your area is created and it contains at least two perimeter doors, you can apply an interlock logic to it so that only one door can be open at a time.

Do the following:

Create and configure a secured area to apply the interlocking logic to.

Link at least two perimeter doors to your area.

For interlock logic to work, the door sensors must be able to detect when the door is opened.

To interlock the perimeter doors of an area:

1. From the **Config Tool** home page, open the **Area view** task.
2. Select the secured area, and click the **Advanced** tab.
3. Set **Interlock** to **ON**.

When set to **ON**, only one perimeter door of the area can be open at any given time. To open a door, all others must be closed.

4. If the door is controlled by an HID unit, set **Antipassback** to **OFF**.
5. Set the following:
 - **Override**: Select the input that is wired to the override key switch or flip switch. When the switch is on, the interlock feature is disabled.
 - **Lockdown**: Select the input that is wired to the lockdown key switch or flip switch. When the switch is on, all perimeter doors remain locked until the switch is back to its normal position.
 - **Priority**: When both the override and lockdown inputs are configured, select which one has priority when both inputs are active.
6. Click **Apply**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 278 of 430

”

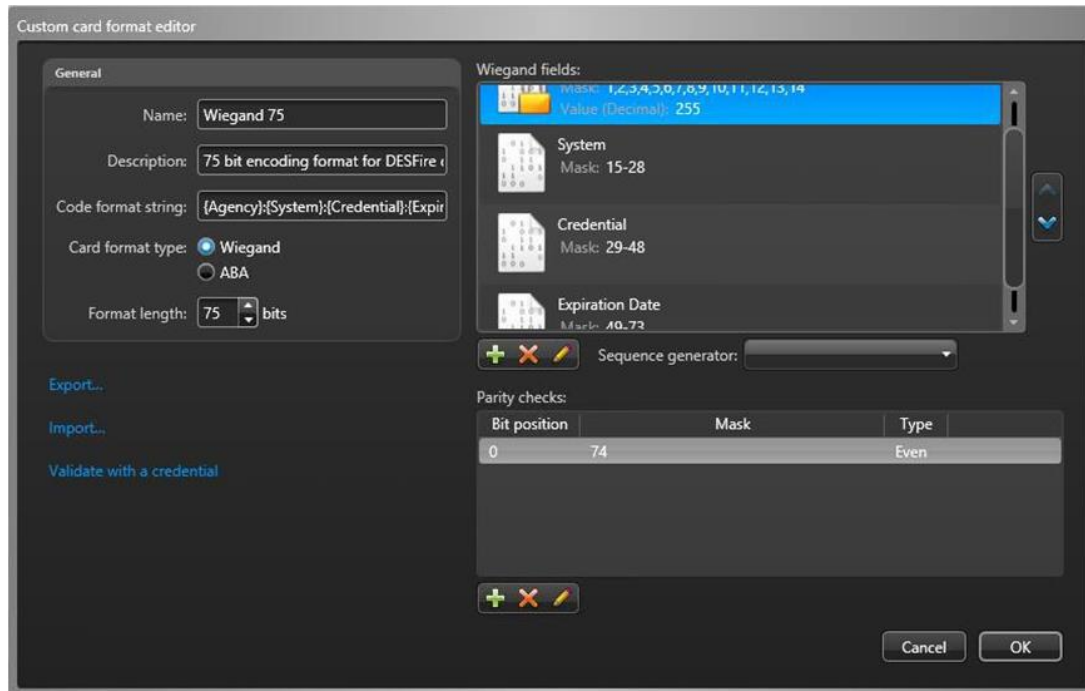
[“Add Custom Card Formats”](#)[“Custom Card Format Editor](#)

Figure 171. Custom Card Format Editor

To navigate to the Custom Card Format Editor:

Go to **Config Tool > Access Control task > General settings > Custom Card Formats**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 279 of 430

Importing Custom Card Formats

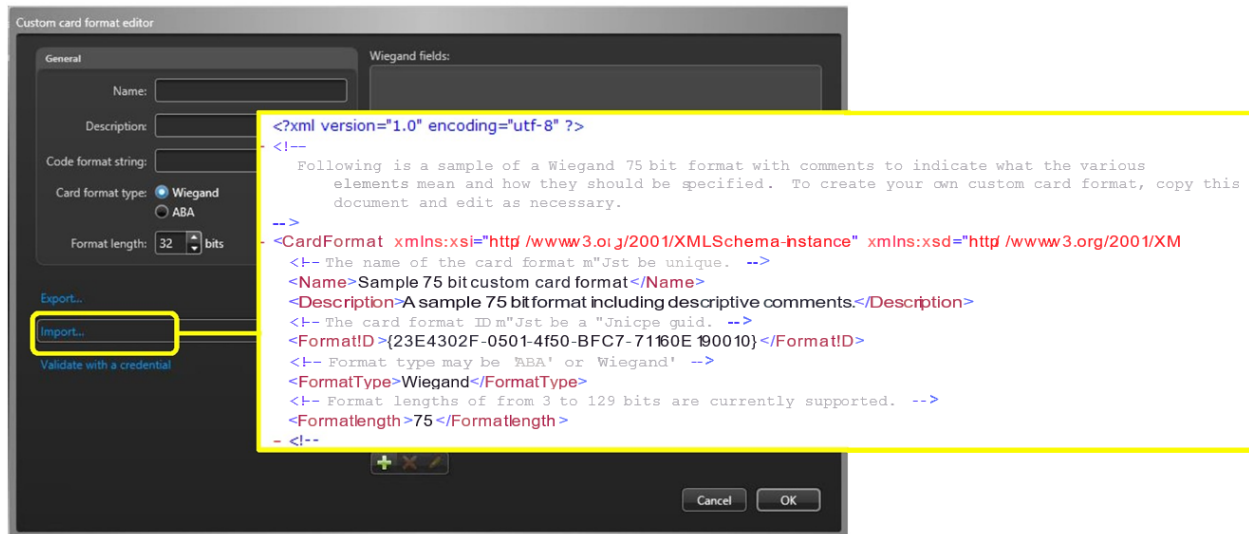


Figure 172. Importing Custom Card Formats

Above is a sample of a Wiegand 75 bit format with comments to indicate what the various elements mean and how they should be specified. To create your own custom card format, copy this document and edit as necessary.

```
-- >
<CardFormat xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
/www.w3.org/2001/XM
<!-- The name of the card format must be unique. -->
<Name>Sample 75 bit custom card format</Name>
<Description>A sample 75 bit format including descriptive comments.</Description>
<!-- The card format ID must be a "Jnicpe guid. -- >
<FormatID>{23E4302F-0501-4f50-BFC7-71160E190010}</FormatID>
<!-- Format type may be 'ABA' or 'Wiegand' -- >
<FormatType>Wiegand</FormatType>
<!-- Format lengths of from 3 to 129 bits are currently supported. - - >
<Formatlength>75</Formatlength>
<!--
```

See [Badge Designer](#).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 280 of 430

3.11.5.13 Custom Card Formats

In addition to the standard card formats that are supported in Security Center, you can define custom card formats with unique data fields.

You can define custom card formats in Config Tool from the General settings view in the Access control task.

Benefits of custom card formats

Creating custom card formats has the following benefits:

You can manually enroll a new card using a standard workstation keyboard, whereas a card with an unknown format can only be enrolled using a card reader.

You can view the card number in the **Config Tool** and the *Security Desk*, whereas data for unknown card formats cannot be displayed.

You can import cards using custom formats with the **Import** tool.

You can enroll cards automatically, with a card reader, or manually in bulk, without a card reader, using the **Credential management** task.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 281 of 430

3.11.5.14 Custom Card Format Editor Tool

The custom card format editor is a *Synergis*™-specific tool that allows you to define your own card formats. It is available from the **General settings** view in the **Access control** task.

Only administrative users can use this tool.

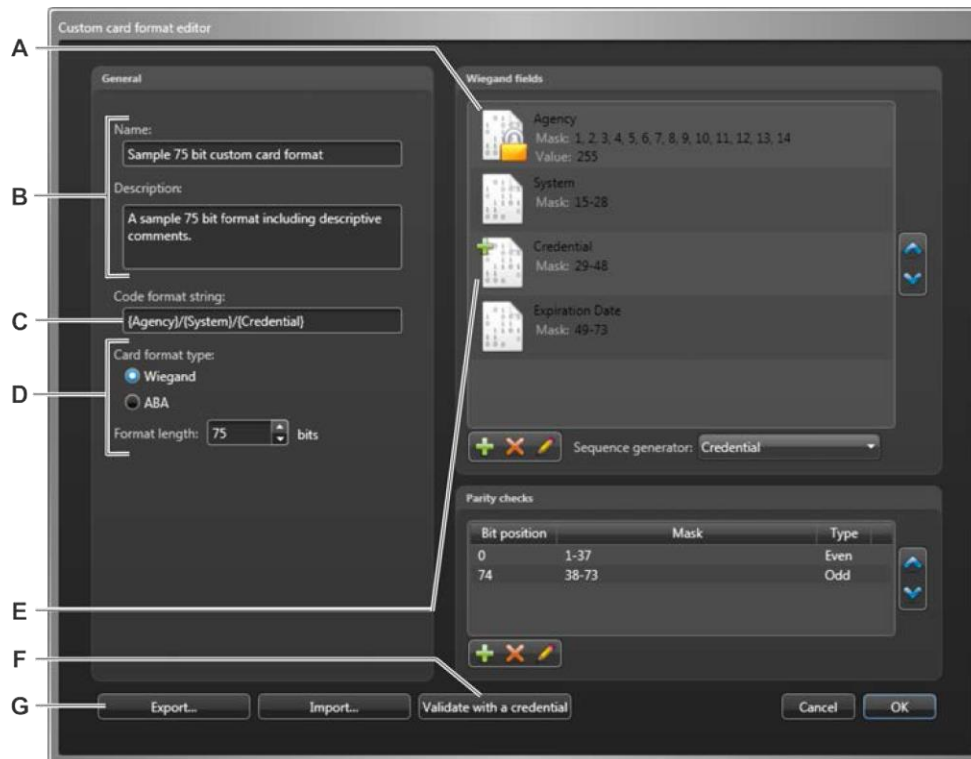


Figure 173. Custom Card Format Editor Tool

- A. Fixed value field (indicated by the padlock (🔒) icon).
- B. Card format name and description listed in the **Access control task, view**.
- C. Format used to display the **Credential code** in reports.
- D. Select the card format type and length before defining the fields.
- E. Field designated as the sequence generator (indicated by the plus (+) icon).
- F. Validate the format with pre-enrolled credentials.
- G. Import/export card format from XML file.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 282 of 430

3.11.5.15 Creating Custom Card Formats

To define custom card formats that have unique data fields, you can create custom formats manually, or import them from XML files, using the **Custom card format editor** tool.

If you delete a custom card format that is being used in *Security Center*, all credentials using that format appear as *Unknown*, but the credentials are still granted access at the doors.

NOTE: You need to know the format of your card to enter it into the credential code field. If you do not know the format of your card, contact the card manufacturer or your sales representative of Genetec™ Inc. for help.

To create a custom card format:

1. Open the **Access control** task, and click the **General settings** view.
2. Under **Custom card** formats, click **Add an item** (+).
3. In the **Custom card format** editor, enter the **Name** and **Description** of the custom card format.
4. Specify the **Card format type** and **Format length**.

- Wiegand (8 to 128 bits)
- ABA (2 to 32 characters)

5. Define the *Wiegand* fields or define the *ABA* fields that constitute the custom card format.
6. If you selected *Wiegand* format type, you might have to add parity check bits to the format.
7. (*Wiegand* type only) If you want to enroll a range of credentials in bulk, you can designate one field as the sequence generator.

The field designated as the sequence generator allows you to define a range of values for enrolling the credentials in bulk in the **Credential Management** task.

8. Enter the **format** string for printing the **credential** code.

The credential code is the printed form of the **credential** data. It is an optional column that is available in most access control related reports. The **Code format** string tells the system how to print the credential data. To include a field in the credential code, the field name must be specified in the **code format** string as it is spelled in the card format field definition, between curly brackets "{ }". The field names are case-sensitive. Any other characters in the format string that are not found between curly brackets are printed as is. For example, with the format string "{Facility}/{Card Number}", a credential with the respective field values 230 and 7455 will be printed as "230/7455".

9. To validate the new custom card format with a pre-enrolled credential, click **Validate** with a credential, select a **pre-enrolled** credential, and click **OK**.
10. (Optional) Click **Export** to save the custom card format to an XML file.

Exporting the custom card format to an XML file allows you to import that same card format definition to other Synergis™ systems.

11. Click **OK > Apply**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 283 of 430

[Import Tool](#)[“Custom Fields”](#)[“Global Cardholder Synchronization”](#)

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 284 of 430	

3.11.5.16 Import Cardholders from Active Directory

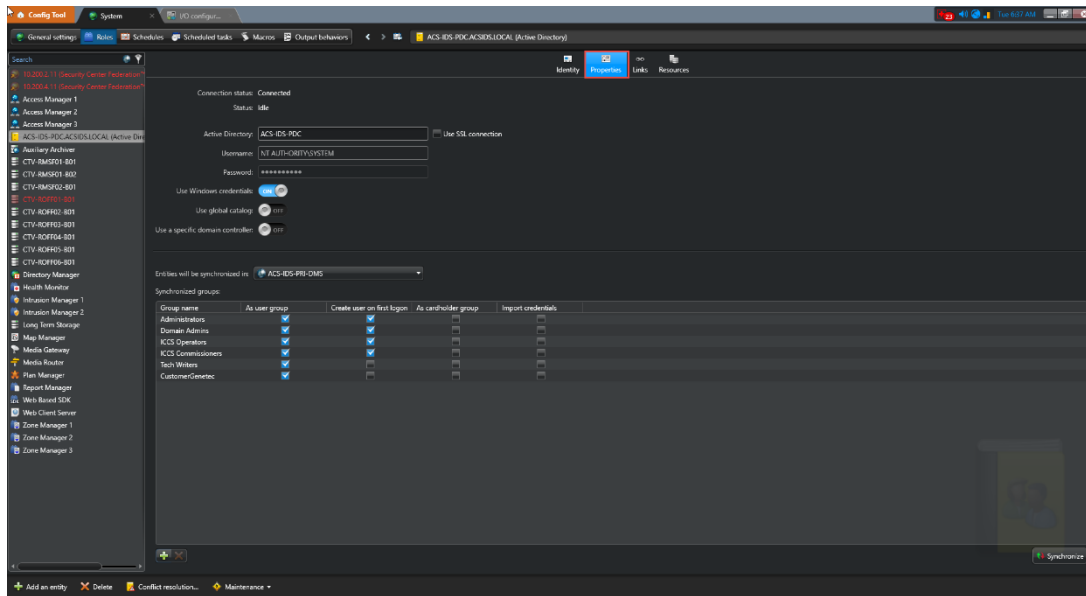


Figure 161. Access Control Configuration: Roles: Import Cardholders from Active Directory

Integrating a Windows Active Directory (AD) into Security Center allows you to manage all personnel and security information from a single location, whether it is for logical security (IT) or for physical security (controlling access to physical locations).

With AD integration, you can import security groups from an AD into Security Center as user groups, cardholder groups, or both. Members can be imported as users or cardholders. Both standard and custom attributes can be imported from the AD. Most imported fields can only be modified within the AD and are read-only in Security Center.

You can import entities from more than one AD if necessary. For example, from Security Center, you can manage access to a facility shared by multiple companies, such as an office building. As system administrator, you can import users and/or cardholders from their individual Active Directories, and manage them in separate partitions.

For larger AD setups that have many domains that are part of an AD forest, Security Center supports synchronizing Universal groups and connecting to a global catalog. A single Active Directory role can be used to synchronize a universal group. For more information about using Universal groups and global catalogs with Security Center, see [About Universal Groups and Global Catalogs](#).

NOTE: Make sure that the server running the Active Directory Role is part of the domain that you are trying to synchronize.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 285 of 430

3.11.5.17 How AD Integration Works

To import users and/or cardholders from an AD, you must create an **Active Directory** role for the AD you want to import. The **Active Directory** role connects your *Security Center* system to an Active Directory server, and imports users and/or cardholders from selected security groups. Imported entities are identified in *Security Center* by a yellow arrow (👉) superimposed on the regular entity icon.

The **Active Directory** role synchronizes all the changes made on the AD with the imported entities in *Security Center*. It also pushes the logon credentials of imported users to the AD service for validation.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 286 of 430	

3.11.5.18 Benefits of AD Integration

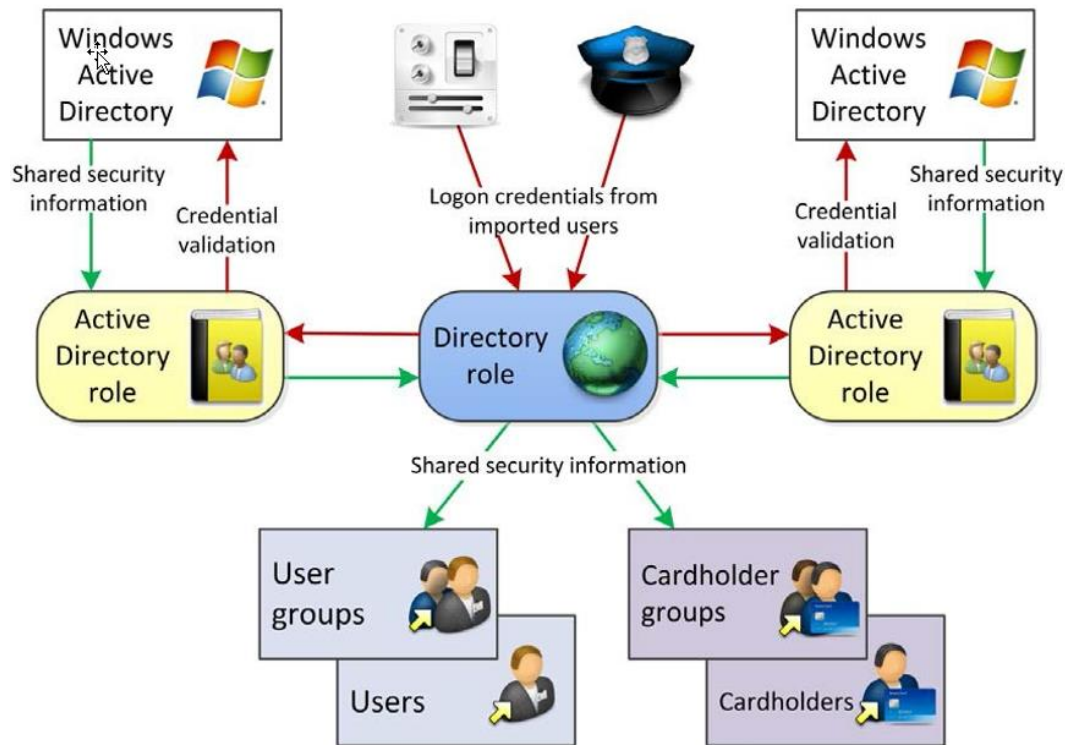


Figure 162. Benefits of Active Directory Integration

Having a centralized security information management system provides many benefits:

Less data entry means fewer errors and better control during initial *Security Center* setup, because users and cardholders can be imported from an existing AD.

Consistency and better security because all shared information is entered only once.

- A new user account that is added to an imported security group automatically adds a new user and/or cardholder in *Security Center*.
- A user account that is disabled in the AD automatically disables the corresponding user and/or cardholder in *Security Center*.

Single logon capability for synchronized *Security Center* users. Users logged on to Windows do not have to log on to *Security Center*.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 287 of 430

3.11.5.19 Active Directory Synchronization

Through a process called synchronization, the **Active Directory** role also keeps all imported entities up-to-date with changes made on the AD.

All imported entities are synchronized with their source by the **Active Directory** role. Most of the attributes imported from the AD are read-only in *Security Center*, except for a few cardholder properties. Imported entities cannot be deleted unless they are deleted from the AD.

CAUTION: If you move a security account from a synchronized AD security group to one that is not synchronized, it is as though the account ceases to exist in *Security Center*. The Active Directory role deletes the corresponding entities (users and/or cardholders) from *Security Center* the next time it synchronizes with the AD.

Synchronization is always initiated from *Security Center*. There are two ways that you can start synchronization:

- **Manually:** Synchronization is performed when you explicitly request it. This is the default setting. The advantage of this approach is that you have perfect control over when you want the synchronization to be done.

- **On schedule:** The imported groups are synchronized using a scheduled task.

Information that can be synchronized with the AD

Both standard and custom *Security Center* fields can be imported from the AD, and kept synchronized with the AD. You can choose which user group, user, cardholder group, and cardholder fields to import from the AD in the Links tab of the **Active Directory** role.

The standard attributes you can import from the AD are:

User group

- Name
- Description
- Email address
- All group members (users)

User

- Membership in the imported user group
- Username
- Password
- Description
- First name
- Last name
- Email address
- Status: Active or Inactive

• Cardholder group

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 288 of 430

- Name
- Description
- Email address
- All group members (cardholders)
- **Cardholder**
 - Membership in the imported cardholder group
 - Cardholder name
 - Description
 - First name
 - Last name
 - Email address
 - Status: Active or Inactive
 - Picture (optional through the Links tab)
 - Partition (optional through the Links tab)

Credential

- Association to the imported cardholder
- Credential name
- Card data
- Card format
- Facility code
- Card number
- Status: Active or Inactive
- Partition (optional through the Links tab)

Additional attributes are imported from the AD by mapping them to *Security Center* custom fields. The **Active Directory** role keeps all imported fields synchronized with the AD.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 289 of 430

3.11.5.20 About Universal Groups and Global Catalogs

Security Center supports synchronizing Universal groups that belong to a global catalog. Users from different domains in an AD forest can access *Security Center* using one **Active Directory** role connected to one domain controller (global catalog). There are some things you should know before synchronizing a Universal group that belongs to a global catalog.

Note the following when importing a Universal group that belongs to a global catalog:

There must be a trust relationship configured between all domains in the AD forest.

Primary groups are not supported.

In order to retrieve the directories within a forest, the Active Directory role user must be able to read the *CN=Partitions*, *CN=Configuration*, *DC=ROOTDOMAIN*, *DC=COM* folder.

If you are importing a Universal group that does not belong to a global catalog:

- The **Active Directory** role contacts several ADs. The **Active Directory** role user must have the necessary permissions to access the different ADs within a forest.
- The default port used to contact the AD is 389. If you are using a different port, you must append it to the AD server name defined in the **Active Directory** field on the **Properties** tab, for example: **ADServer.Genetec.com:3393**.

If you are importing a Universal group that belongs to a global catalog:

- The global catalog must be updated to include the attributes required for *Security Center* user and cardholder information. For the list of required attributes, see [Global Catalog Attributes](#).
- The default port used to contact the AD is 3268. If you are using a different port, you must append it to the AD server name defined in the **Active Directory** field on the **Properties** tab. The name and port number must be separated by a colon, for example:
ADServer.Genetec.com:3295.

Benefits of using a global catalog

A global catalog stores a copy of all AD objects in a forest which provides many benefits:

The need to query multiple domains for information is eliminated since everything is stored in the global catalog.

Less time to process information.

Less bandwidth used.

Less replication of information.

Requires only a single **Active Directory** role connection. All users can access *Security Center* using the global catalog.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 290 of 430

3.11.5.21 Importing Security Groups from an Active Directory

To have a centralized personnel management system, you can import AD security groups into Security Center as user groups or cardholder groups.

If you are importing a universal group from a global catalog, read About universal groups and global catalogs.

When importing an AD security group, you must import all members of that group, including the subgroups. If you want to import only a subset of its members, for example, only *Security Center* users, you must define a new AD security group with only the members you want to import.

If you are integrating multiple ADs into *Security Center*, they must each belong to a different domain.

If you have servers in your system that are running an earlier version of *Security Center*, you must upgrade the servers to the current version before using them to host a new **Active Directory** role.

- An AD security group can be imported as user group, cardholder group, or both.

To import a security group:

12. Open the **System** task, and click the **Roles** view.
13. Click **Add an entity** (+) and select **Active Directory**.
14. On the **Specific info** page, do the following:
 - G. (If you have multiple servers in your system) From the **Server** drop-down list, select the server on which you want to host the role.
 - H. In the **Active Directory** field, enter the AD Fully Qualified Domain Name (FQDN), hostname, or IP address of the AD server.

If you are not using a default port, you must append the port number you are using to the AD server name, separated by a colon. For example, **ADServer.Genetec.com:123**. The default ports are as follows:

- Active Directory with no SSL: 389
 - Active Directory with SSL: 636
 - Global catalog no SSL: 3268
 - Global catalog with SSL: 3269
- I. Specify how you want the role to connect to the AD server. You must have read access to the selected AD service.
 - Use the Windows credentials assigned to the *Genetec™ Server* service that is running on the server hosting the **Active Directory** role.
 - Specify a different set of Windows credentials (username, password).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 291 of 430

15. On the **Basic information** page, enter the name, description, and partition where you want to create the **Active Directory** role.
16. Click **Next**, **Create**, and **Close**.

A new **Active Directory** role (🔑) is created. Wait a few seconds for the role to connect to the AD server.

17. (Optional) If you are importing a universal group that connects to a global catalog, turn on the **Use global catalog** option.
18. On the **Properties** tab, select the AD security groups you want to import.

NOTE: There are two types of groups in Windows Active Directory: distribution groups and security groups. Security Center can only synchronize with security groups.

J. Click **Add an item** (+).

K. Select the security groups you want to add to your **Active Directory** role. Use one of the following methods:

- (Recommended) Type the name of the group in **Find Active Directory** groups, and click (🔍).

If the text you entered matches a single group, it is automatically added to the **Selected groups** list.

If the text you entered matches multiple group names, a second dialog box appears listing all the group names that match the text you entered.

Select the ones you want, and click **OK** to add them to the **Selected groups** list.

- From the **Selected groups** list, click (+).

The **Active Directory members** dialog box appears.

Select a security group, and click **OK**. Only security groups can be synchronized. If you selected an item that is not a security group, the **OK** button remains disabled.

NOTE: The names shown in the dialog box are display names. *Security Center* only synchronizes the account names because they are guaranteed to be unique. Typically, the display names and the account names are the same. The only way to tell them apart is that the display names contain spaces.

- L. Repeat the previous step as often as necessary until all security groups you want to synchronize with the AD are listed in **Selected groups**, and then click **OK**.

The selected groups are listed under **Synchronized groups** in the **Properties** tab.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 292 of 430

19. For each of the synchronized groups, specify how you want to import them.

Group name	As user group	Create user on first logon	As cardholder group	Import credentials
Technical Writers	☒	☐	☒	☒
Project Management	☒	☐	☐	☐
Sales Engineering	☒	☒	☐	☐
Hardware Engineering	☐	☒	☒	☒
System Engineering	☐	☒	☒	☒

⚠ No scheduled task exists to synchronize this role. Synchronize now

Figure 163. Synchronized Groups

The following options are available:

- **As user group:** Select this option to import the synchronized group as user group, and the group members as users.
- **Create user on first logon:** This is the default option, and it creates an empty user group. User entities are only created when someone tries to logs on the first time. This option avoids having to create all user entities simultaneously, which can freeze up the system. If you clear this option, all user entities are created at the same time as a user group.
- **As cardholder group:** Select this option to import the synchronized group as cardholder group, and the group members as cardholders. All synchronized cardholders are created simultaneously.
- **Import credentials:** Select this option to import the credential information of the synchronized cardholders.

20. If you are importing the AD security group as cardholder group, select which cardholder fields you want to synchronize with the AD.

21. (Optional) Map custom fields to synchronize with the AD.

22. Click **Apply**, and then click **Synchronize now** (🔄).

All synchronized groups and their members are imported as *Security Center* entities according to your specifications, with a yellow arrow (👉) superimposed on their icon.

After you finish

Some additional configuration might be required, depending on what you synchronized with the AD:

If you already had entities configured in your system, you might need to resolve certain conflicts due to the import.

(Optional) Configure the imported user groups with proper privileges and security options, so that when new user entities are created, they can automatically inherit these properties from their parent user group.

(Optional) Configure the imported cardholders and cardholder groups.

(Optional) Create a scheduled task to synchronize imported entities with the AD on a regular

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 293 of 430

basis.

After you create a scheduled task, the warning message **No scheduled task exists to synchronize this role** disappears from the **Properties** tab.

DRAFT

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 294 of 430	

3.11.5.22 Mapping Custom Fields to Synchronize with Active Directory

In addition to default attributes, you can import other attributes from the AD by mapping them to *Security Center* custom fields. The custom field mapping can be different for each **Active Directory** role in your system.

Make sure that the workstation where **Config Tool** is running is on the same network domain as the AD server.

Define the custom fields that will receive data from the AD.

No more than 32 custom fields can be mapped to the AD.

To map custom fields to synchronize with Active Directory:

23. From the **Links** tab of the **Active Directory** role, under **Custom fields**, click **Add an item** (+).

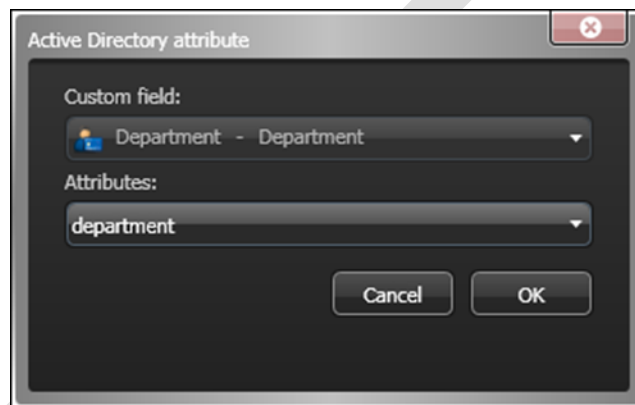


Figure 164. Active Directory Attribute

24. Select the custom field and the AD attribute, and then click **OK**.

IMPORTANT: The data type of the custom field must match that of the AD attribute: text with text, decimal with decimal, date with date, etc. The Security Center image data type must be mapped to the AD binary data type, and the mapped AD attribute must contain a valid JPEG image.

The new mapping appears in the **Links** tab.

25. Repeat the previous steps as needed.
26. Click **Apply**.

The mapped custom fields are displayed in the **Links** tab. When you synchronize with the AD, they are read-only.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 295 of 430

3.11.5.23 Resolving Conflicts Caused by Imported Entities

Conflict resolution might be necessary if you have existing entities (users or cardholders) in your database before importing entities from the AD.

When a synchronized entity has the same name as a local entity, the Active Directory role sees it as a potential conflict. You can use the Conflict resolution tool to view potential conflicts (🔍) and resolve them by deleting the conflicting entities in the the Cardholder Management task.

To resolve conflicts caused by imported entities:

27. Open the **System** task, and click the **Roles** view.

28. Select the Active Directory role (🔍), and click Conflict resolution (🔍).

The **Active Directory conflict resolution** dialog box opens. All synchronized entities are listed to the left. The ones that conflict with a local entity are flagged in green.

29. Resolve each cardholder conflict:

M. Open the **Cardholder Management** task and find the two cardholder records that are in conflict.

N. Select one of the conflicting cardholder records and click **Modify**.

O. Add any missing information that is available in the duplicate cardholder record.

P. Save and close the cardholder record.

Q. Select the duplicate cardholder record and click **Delete Cardholder**.

30. Resolve each user conflict:

R. Open the **User Management** task.

S. In the entity browser, find the two user records that are in conflict.

T. Open one of the conflicting user records.

U. Add any missing information that is available in the duplicate user record.

V. Click **Apply**.

W. Select the duplicate user record and click **Delete**.

5 Return to the **Roles** view in the **System** task.

6 In the **Active Directory conflict resolution** dialog box, select the entities that are flagged as being in conflict and press **Delete**.

7 In the **Active Directory conflict resolution**, click **Finish**.

This process will generate a file named **Conflict_Manifest data** that documents resolved conflicts. It can be saved for future reference.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 296 of 430

3.11.5.24 Deactivating Users Imported from an Active Directory

If you have users that are imported from an Active Directory, you can set the user's status to inactive. The user becomes desynchronized from the AD until you activate the user again.

To deactivate a user imported from an Active Directory:

31. Open the **Security** task.
32. Select an imported user (👤), and click the **Properties** tab.
33. Set the **User status** option to **Inactive**.
34. Click **Apply**.

The user is no longer synchronized with the AD. It will only become synchronized again once you set the user's status to **Active**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 297 of 430	

3.11.5.25 Global Catalog Attributes

For the Active Directory role to successfully connect to a global catalog and synchronize users and cardholders in Security Center, the global catalog must be updated to include specific attributes.

User attributes

The global catalog must be updated with the following user attributes:

distinguishedName
objectGUID
objectClass
cn
objectSid
sAMAccountName
displayName
name
mail
description
userPrincipalName
userAccountControl
accountExpires
givenName
sn
tokenGroup
memberOf (For the SDK only)
any attributes to be used in the **Links** tab

Group attributes

The global catalog must be updated with the following group attributes:

distinguishedName
objectGUID
objectClass
cn
objectSid
sAMAccountName
name
mail

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 298 of 430

description

groupType

member

Container, domain, and organizational unit attributes

The global catalog must be updated with the following container, domain, and organizational attributes:

distinguishedName

objectGUID

objectClass

objectSid

displayName

name

member

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 299 of 430

3.11.5.26 Areas: Antipassback and Interlocking

Antipassback is an access restriction placed on a secured area that prevents a cardholder from entering an area that they have not yet exited from, and vice versa.

Example: After gaining access to a secured area, a cardholder "passes back" his or her credential to an unauthorized individual, who then uses the same credential to access the same area.

A strict antipassback is an antipassback option. When enabled, a passback event is generated when a cardholder attempts to leave an area that they were never granted access to. When disabled, Security Center only generates passback events for cardholders entering an area that they never exited.

Global antipassback is a feature that extends the antipassback restrictions to areas controlled by multiple *Synergis*™ units.

An interlock (also known as sally port or airlock) is an access restriction placed on a secured area that permits only one door to be open at any given time.

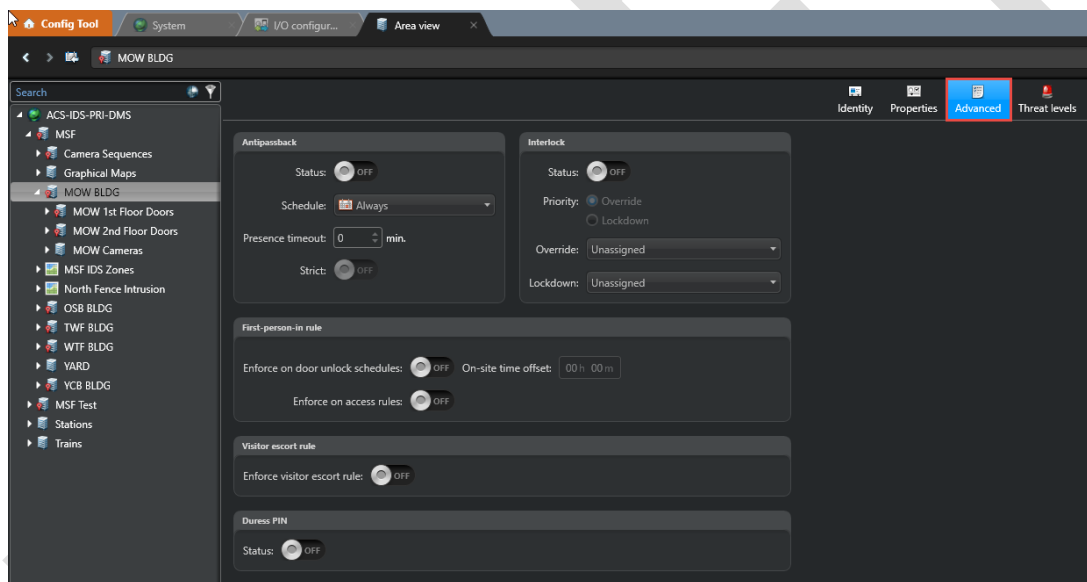


Figure 165. Access Control Configuration: Areas: Antipassback and Interlocking

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 300 of 430

3.11.5.27 Applying Antipassback to Areas

Once your area is created and it contains at least one perimeter door, you can apply antipassback to prevent cardholders from entering areas they have not yet exited, and vice versa.

Create and configure a secured area to apply the antipassback restriction to.

An area enabled with antipassback must be controlled by a single unit. If the area is not controlled by a single unit, the following criteria must be met in order to apply antipassback.

All units controlling the doors within the area are *Synergis™* units.

All units controlling the area are managed by the same Access Manager role.

Global antipassback is enabled on the Access Manager role.

Limitations: For areas controlled by HID units, the antipassback logic is only applied to perimeter doors, not to captive doors.

To configure antipassback for an area:

1. From the **Config Tool** home page, open the **Area view** task.
2. Select the secured area, and click the **Advanced** tab.
3. Set **Antipassback** to **ON**.
4. If the doors are controlled by an HID unit, set Interlock to **OFF**.
5. Set the following:
 - **Schedule:** Select Always if you want antipassback to be applied at all times.
 - **Type:** Type of antipassback to apply.
 - **Soft:** Soft antipassback only logs the passback events in the database. It does not restrict the door from being unlocked due to a passback event.
 - **Hard:** Hard antipassback logs an entry in the database and prevents the door from being unlocked due to a passback event.
 - **Presence timeout:** Set how many minutes a cardholder's presence in the area is remembered for the purpose of passback detection (not used for counting people). Past that period, a cardholder who never left the area can re-enter without triggering a passback event. The default value of zero (0) minutes means that a cardholder's presence never times out.

NOTE: When global antipassback is enabled, the presence of a cardholder in an area is forgotten after seven days if no entry or exit from this area is reported for that cardholder during that period. This means that cardholders can re-enter an area that they never left, or leave an area they never entered, without triggering a passback event if no movement was registered for these cardholders on that area for seven days. This applies even if the **Presence** timeout is set to infinite (=0).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 301 of 430

- **Strict:** Turn this option on to generate passback events for both types of access violations: when cardholders try to re-enter an area that they never left, and when cardholders try to exit an area that they never entered. Otherwise, the default is set to **OFF** and antipassback logic is only verified on area entrances, and passback events are only generated when cardholders try to re-enter an area that they never left.

BEST PRACTICE: If you choose to enable strict and hard antipassback on an area that is not controlled with turnstiles or similar devices that only allow one person through at a time, grant the **Forgive antipassback violation** privilege to the operators responsible for monitoring this area.

NOTE: With strict antipassback turned off, you can have Card-In/REX-out perimeter doors, but the **Presence timeout** parameter must be configured (> 0). With strict antipassback turned on, all perimeter doors must be configured as Card-In/Card-Out, **Presence timeout** must be set to infinite ($= 0$), and no REX can be configured.

6. Click **Apply**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 302 of 430

3.11.5.28 Enabling Global Antipassback on Access Manager Roles

If the areas on which you want to apply the antipassback restrictions are controlled by multiple *Synergis™* units, you must enable global antipassback on the **Access Manager** roles.

When strict and hard antipassback is applied to an area without global antipassback, a cardholder who entered the area through one door cannot leave the area through another door if both doors are not controlled by the same unit. Also, the same cardholder who entered the area through one door, can re- enter the area through a different door if the two doors are not controlled by the same unit. With global antipassback enabled, these two violations can be prevented.

IMPORTANT: Global antipassback only works on areas that are entirely controlled by *Synergis™* units. All units controlling the same area must be managed by the same Access Manager.

TIP: If you need to switch your units between **Access Manager** roles to meet the global antipassback requirements, use the [Move Unit Tool](#).

To enable global antipassback on an Access Manager role:

7. From the **Config Tool** home page, open the **Access control** task, and click the **Roles and units** view.
8. Select the **Access Manager** role to configure, and click the **Properties** tab.
9. On the **Properties** page, select the following options: **Enable peer to peer** and **Enable global antipassback**.

NOTE: Up to 15 *Synergis™* units can be connected as peers.

10. Click **Apply**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 303 of 430

3.11.5.29 Areas: Interlock

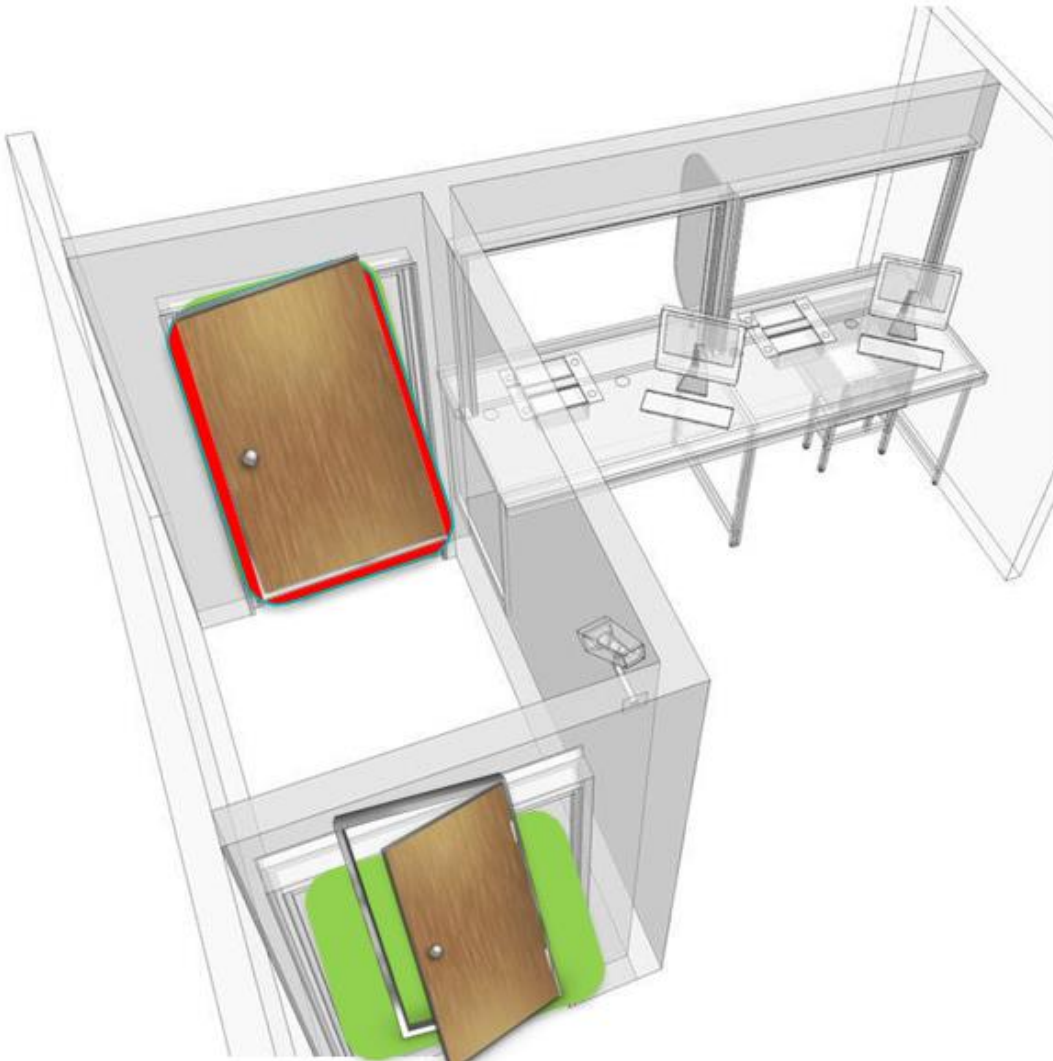


Figure 166. Interlock: Access Granted to 1 Door at a Time

Access is granted one door at a time while access to the interior cannot be accessed without appropriate credentials.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 304 of 430	

3.11.5.30 Areas: Interlock Override

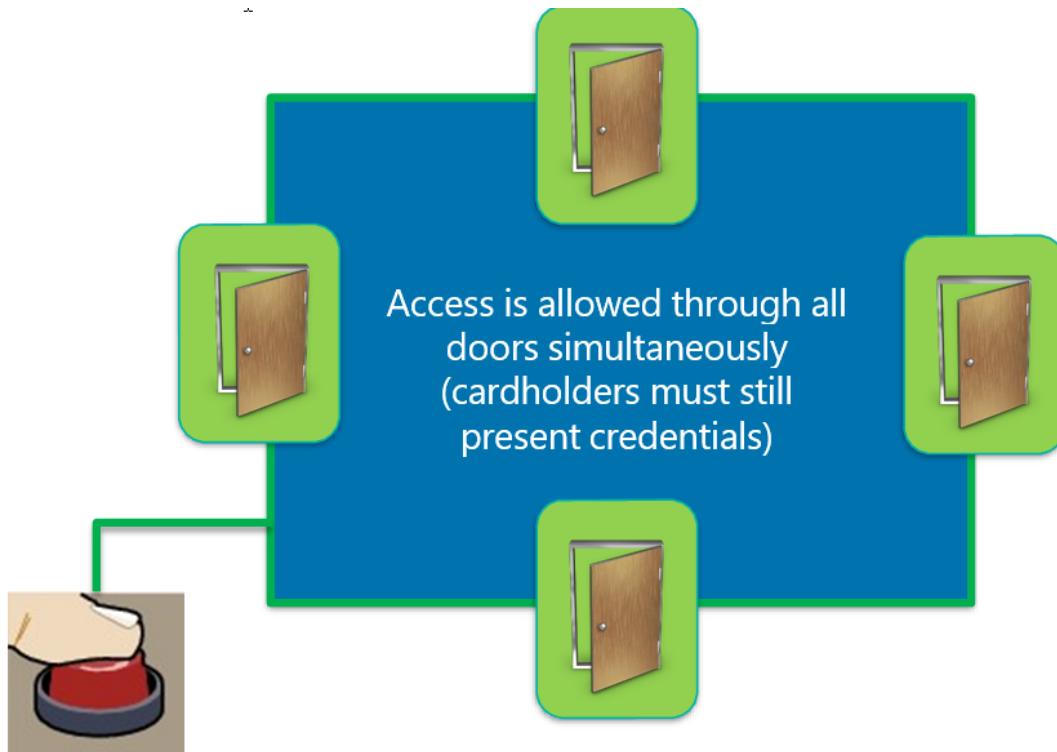


Figure 167. Interlock: Interlock Override

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 305 of 430	

3.11.5.31 Areas: Interlock Lockdown

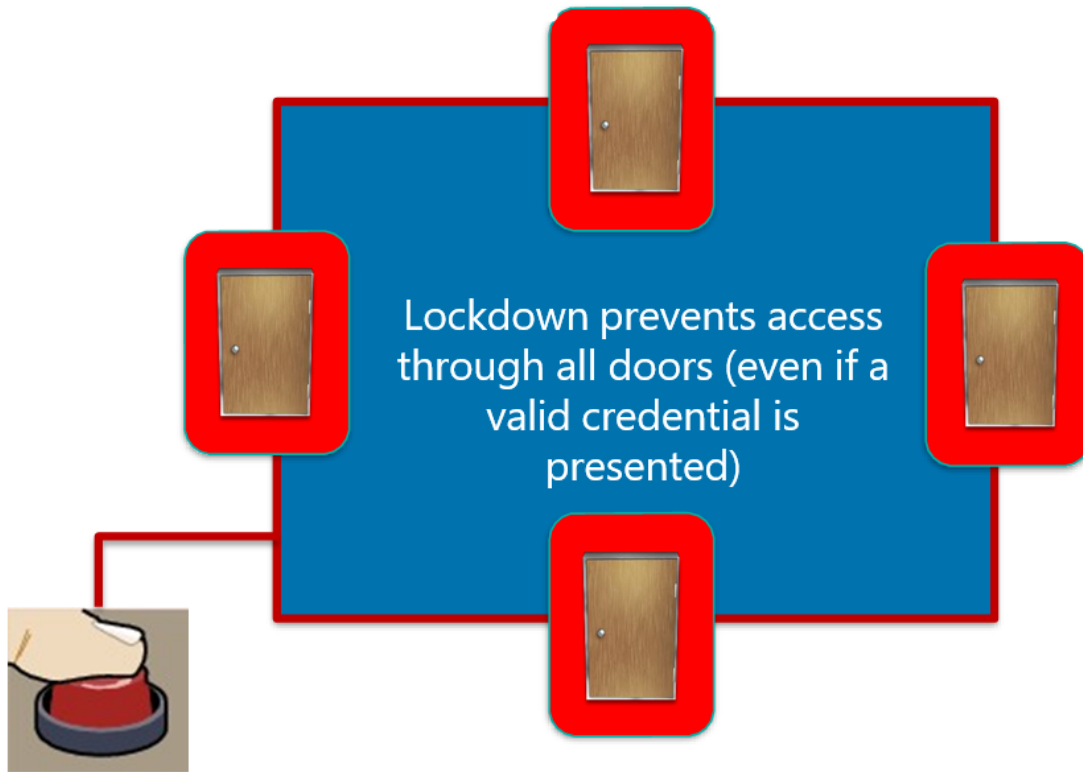


Figure 168. Interlock: Lockdown

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 306 of 430	

3.11.5.32 Interlocking Doors within Areas

Once your area is created and it contains at least two perimeter doors, you can apply an interlock logic to it so that only one door can be open at a time.

Do the following:

Create and configure a secured area to apply the interlocking logic to.

Link at least two perimeter doors to your area.

For interlock logic to work, the door sensors must be able to detect when the door is opened.

To interlock the perimeter doors of an area:

11. From the **Config Tool** home page, open the **Area view** task.
12. Select the secured area, and click the **Advanced** tab.
13. Set **Interlock** to **ON**.

When set to **ON**, only one perimeter door of the area can be open at any given time. To open a door, all others must be closed.

14. If the door is controlled by an HID unit, set **Antipassback** to **OFF**.

15. Set the following:

- **Override:** Select the input that is wired to the override key switch or flip switch. When the switch is on, the interlock feature is disabled.
- **Lockdown:** Select the input that is wired to the lockdown key switch or flip switch. When the switch is on, all perimeter doors remain locked until the switch is back to its normal position.
- **Priority:** When both the override and lockdown inputs are configured, select which one has priority when both inputs are active.

16. Click **Apply**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 307 of 430

3.11.5.33 Add Custom Card Formats

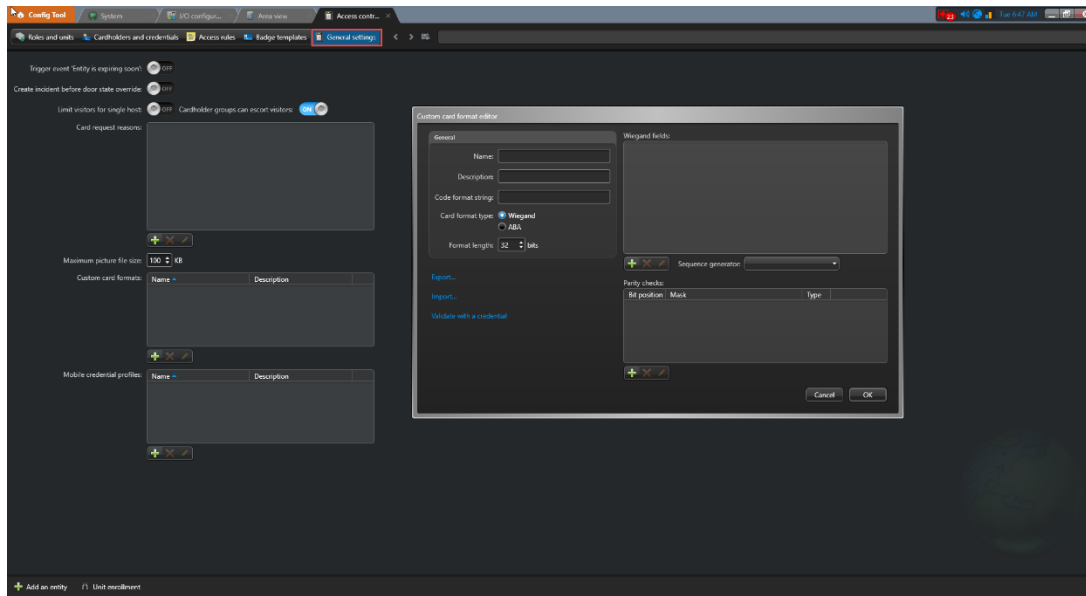


Figure 169. Access Control Configuration: General Settings: Add Custom Card Formats

A custom card format means that the standard bit mapping of which bits map to which fields are switched around so that the card information cannot be properly understood unless we have the “decoding template” to know which bits map to which field.

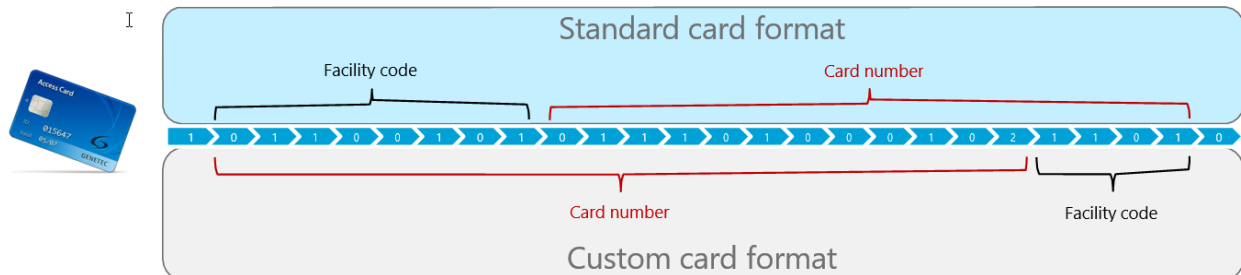


Figure 170. Custom Card Format

A custom card format means that the standard bit mapping of which bits map to which fields are switched around so that the card information cannot be properly understood unless we have the “decoding template” to know which bits map to which field.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 308 of 430

Custom Card Format Editor

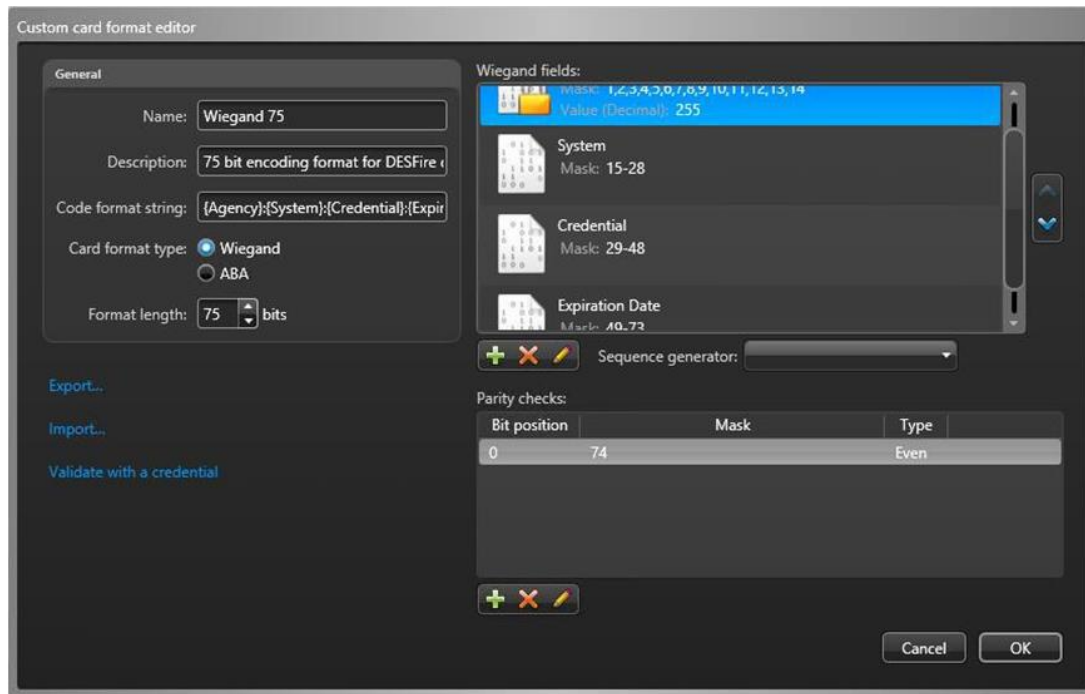


Figure 171. Custom Card Format Editor

To navigate to the Custom Card Format Editor:

Go to **Config Tool > Access Control task > General settings > Custom Card Formats.**

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 309 of 430

Importing Custom Card Formats

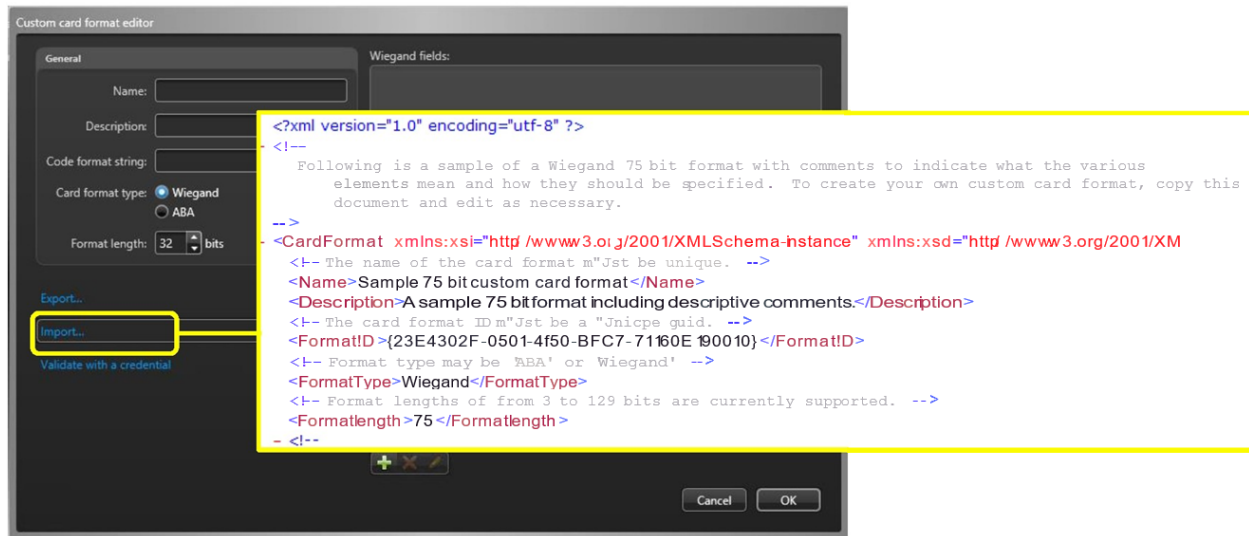


Figure 172. Importing Custom Card Formats

Above is a sample of a Wiegand 75 bit format with comments to indicate what the various elements mean and how they should be specified. To create your own custom card format, copy this document and edit as necessary.

```
-- >
<CardFormat xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <!-- The name of the card format must be unique. -->
  <Name>Sample 75 bit custom card format</Name>
  <Description>A sample 75 bit format including descriptive comments.</Description>
  <!-- The card format ID must be a "Jnicpe guid. -->
  <FormatID>{23E4302F-0501-4f50-BFC7-71160E190010}</FormatID>
  <!-- Format type may be 'ABA' or 'Wiegand' -->
  <FormatType>Wiegand</FormatType>
  <!-- Format lengths of from 3 to 129 bits are currently supported. -->
  <Formatlength>75</Formatlength>
  <!--
```

See [Badge Designer](#).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 310 of 430

3.11.5.34 Custom Card Formats

In addition to the standard card formats that are supported in Security Center, you can define custom card formats with unique data fields.

You can define custom card formats in Config Tool from the General settings view in the Access control task.

Benefits of custom card formats

Creating custom card formats has the following benefits:

You can manually enroll a new card using a standard workstation keyboard, whereas a card with an unknown format can only be enrolled using a card reader.

You can view the card number in the **Config Tool** and the *Security Desk*, whereas data for unknown card formats cannot be displayed.

You can import cards using custom formats with the **Import** tool.

You can enroll cards automatically, with a card reader, or manually in bulk, without a card reader, using the **Credential management** task.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 311 of 430	

3.11.5.35 Custom Card Format Editor Tool

The custom card format editor is a *Synergis*™-specific tool that allows you to define your own card formats. It is available from the **General settings** view in the **Access control** task.

Only administrative users can use this tool.

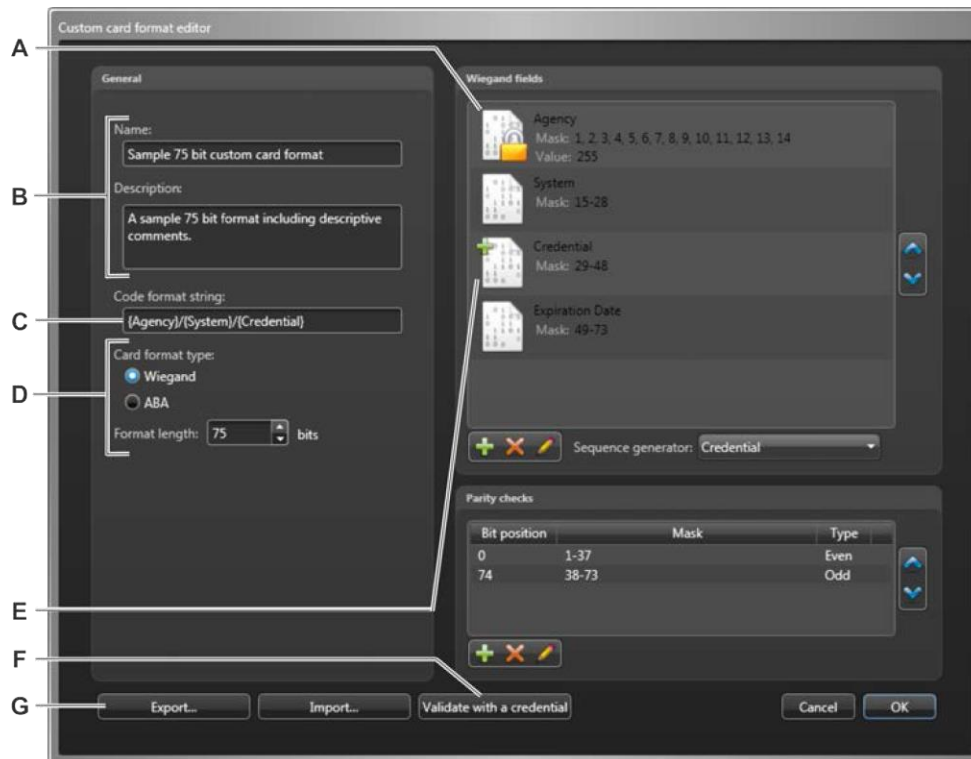


Figure 173. Custom Card Format Editor Tool

- H. Fixed value field (indicated by the padlock (🔒) icon).
- I. Card format name and description listed in the **Access control task, view**.
- J. Format used to display the **Credential code** in reports.
- K. Select the card format type and length before defining the fields.
- L. Field designated as the sequence generator (indicated by the plus (+) icon).
- M. Validate the format with pre-enrolled credentials.
- N. Import/export card format from XML file.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 312 of 430

3.11.5.36 Creating Custom Card Formats

To define custom card formats that have unique data fields, you can create custom formats manually, or import them from XML files, using the **Custom card format editor** tool.

If you delete a custom card format that is being used in *Security Center*, all credentials using that format appear as *Unknown*, but the credentials are still granted access at the doors.

NOTE: You need to know the format of your card to enter it into the credential code field. If you do not know the format of your card, contact the card manufacturer or your sales representative of Genetec™ Inc. for help.

To create a custom card format:

17. Open the **Access control** task, and click the **General settings** view.
18. Under **Custom card** formats, click **Add an item** (+).
19. In the **Custom card format** editor, enter the **Name** and **Description** of the custom card format.
20. Specify the **Card format type** and **Format length**.

- Wiegand (8 to 128 bits)
- ABA (2 to 32 characters)

21. Define the *Wiegand* fields or define the *ABA* fields that constitute the custom card format.
22. If you selected *Wiegand* format type, you might have to add parity check bits to the format.
23. (*Wiegand* type only) If you want to enroll a range of credentials in bulk, you can designate one field as the sequence generator.

The field designated as the sequence generator allows you to define a range of values for enrolling the credentials in bulk in the **Credential Management** task.

24. Enter the **format** string for printing the **credential** code.

The credential code is the printed form of the **credential** data. It is an optional column that is available in most access control related reports. The **Code format** string tells the system how to print the credential data. To include a field in the credential code, the field name must be specified in the **code format** string as it is spelled in the card format field definition, between curly brackets "{ }". The field names are case-sensitive. Any other characters in the format string that are not found between curly brackets are printed as is. For example, with the format string "{Facility}/{Card Number}", a credential with the respective field values 230 and 7455 will be printed as "230/7455".

25. To validate the new custom card format with a pre-enrolled credential, click **Validate** with a credential, select a **pre-enrolled** credential, and click **OK**.
26. (Optional) Click **Export** to save the custom card format to an XML file.

Exporting the custom card format to an XML file allows you to import that same card format definition to other Synergis™ systems.

27. Click **OK > Apply**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 313 of 430

3.11.5.37 Import Tool

See System Tools

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 314 of 430	

3.11.5.38 Custom Fields

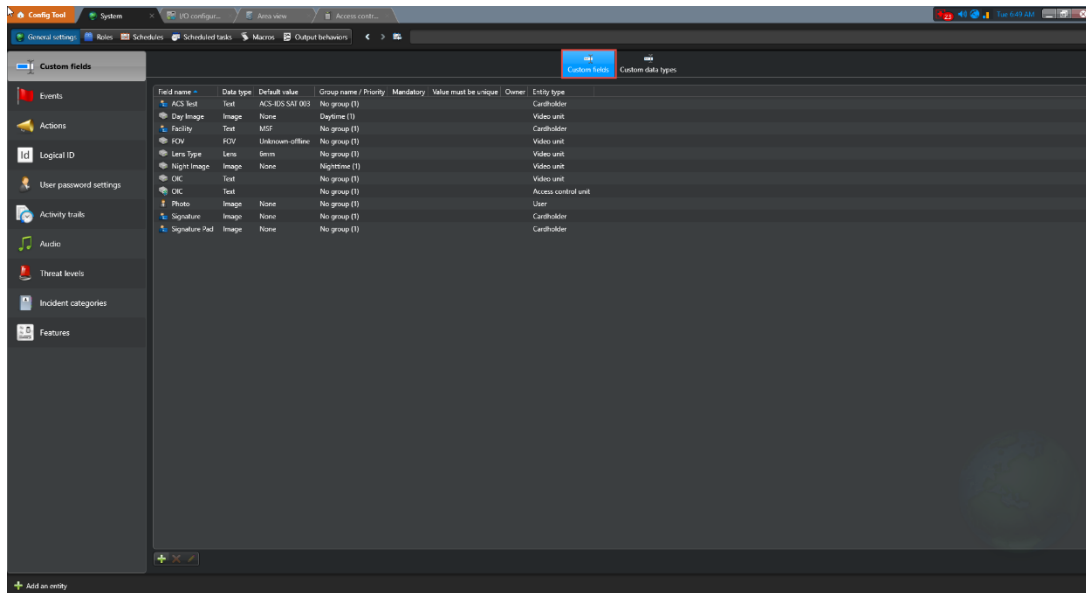


Figure 174. Access Control Configuration: General Settings: Custom Fields

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 315 of 430

3.11.5.39 Global Cardholder Synchronization

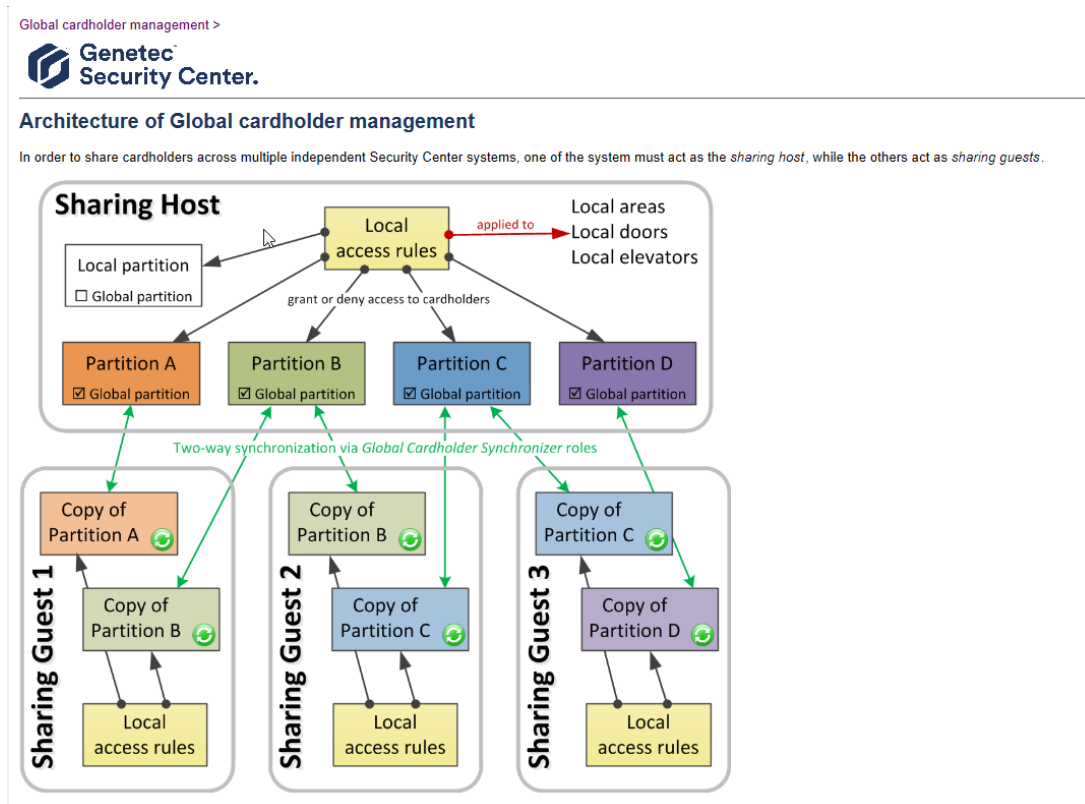


Figure 175. Access Control Configuration: Global Cardholder Synchronization

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 316 of 430

3.11.6 Badge Designer

Badge designer is a tool that allows you to design and modify badge templates.

This section includes:

[“Badge Template”](#)

[“Creating Badge Templates”](#)

[“Badge Template - Badge Designer Tab”](#)

[“Designing Badge Templates”](#)

[“Viewing Print Previews of Badge Templates”](#)

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 317 of 430	

3.11.6.1 Badge Template

A badge template is a type of entity used to configure a printing template for badges.

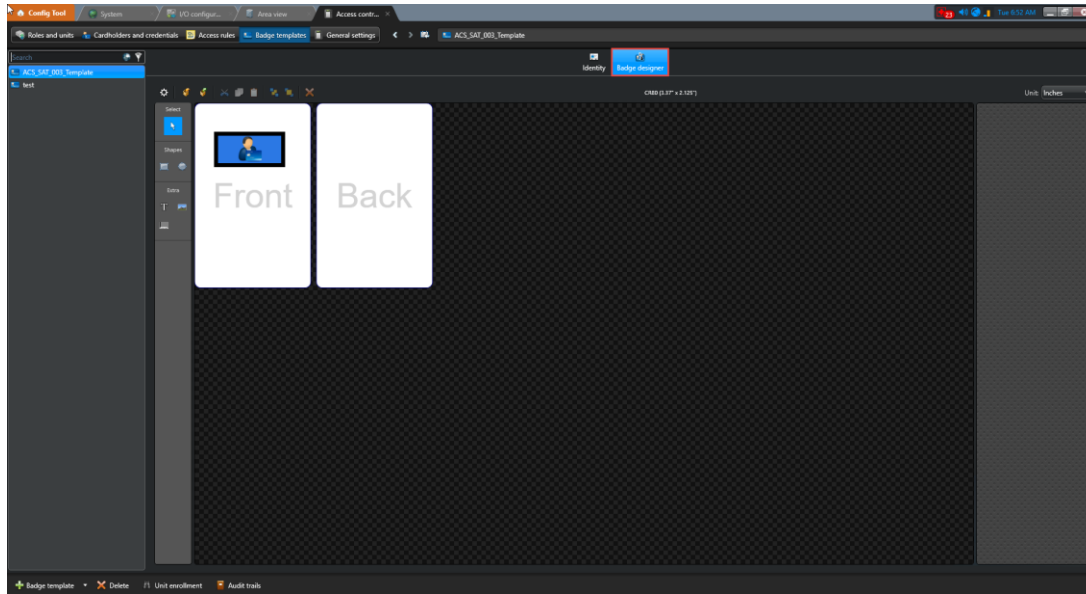


Figure 176. Access Control Configuration: Badge Designer

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 318 of 430

3.11.6.2 Creating Badge Templates

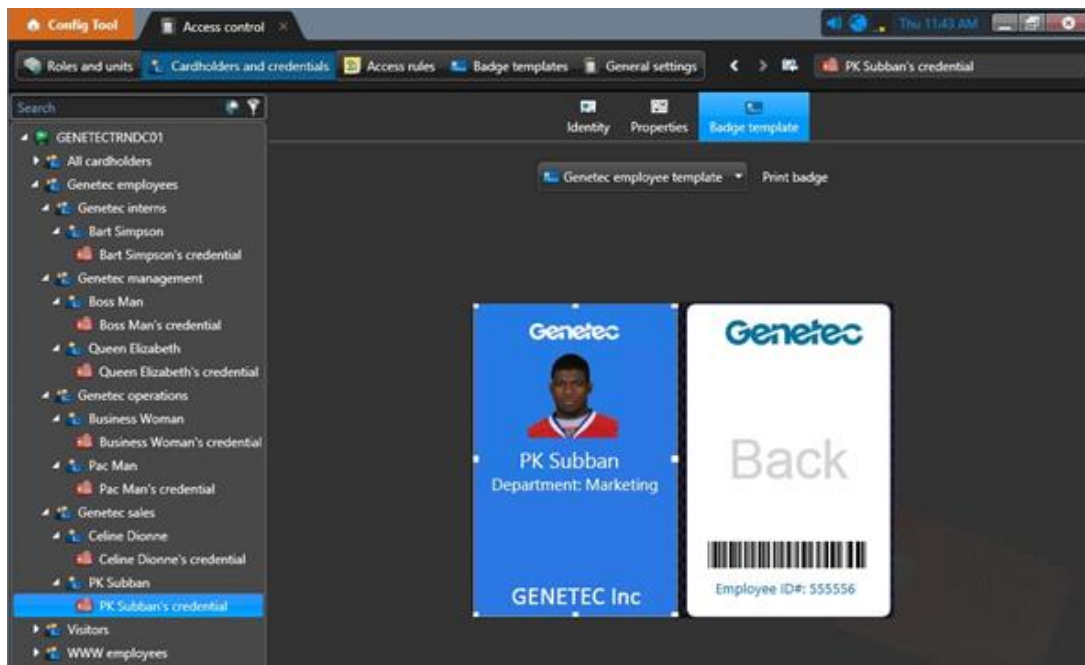


Figure 177. Badge Template

Badge templates can have dynamic values mapped to database fields.

3.11.6.3 Badge Template - Badge Designer Tab

This section lists the settings found in the **Badge template Badge designer** tab, in the **Access control** task.

In the **Badge designer** tab, you can design and modify badge templates. In the **Badge designer**, there are different tools you can use to edit a template.

Tools: In the **Tools** section, there are six graphical tools you can use to edit the template:

Select tool: Use to click and select an object on the template.

Rectangle tool: Use to draw a square/rectangle on the template.

Ellipsis tool: Use to draw circles/ovals on the template.

Text tool: Use to insert text on to the template.

Image tool: Use to insert a picture on to the template.

Barcode tool: Use to insert barcodes on to the template.

Image: In this widget, you can choose whether the image displayed on the badge uses a cardholder picture or an image from a file, and whether the image should be stretched or not.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 319 of 430

Text: In this widget, you can add **cardholder** fields, as well as edit the text, the text color, and the text alignment.

Color and border: In this widget, the following options are available:

Fill: Use to modify the fill color of an inserted object like a square or oval.

Opacity: Use to modify the opacity of an inserted object.

Border: Use to modify the border color of an inserted object.

Border thickness: Use to modify the thickness of the inserted object's border.

Size and position: In this widget, you can choose where the text or image is located on the badge, and its width and height.

Properties (⚙️): Opens the **Format** dialog box, where you can select from the following card sizes and orientation.

- CR70
- CR80
- CR90
- CR100
- Custom card size
- Orientation. You can choose Landscape or Portrait orientation.

Import (📁): Import a badge design that was previously exported from **Config Tool** as a badge template (BDG formats only).

Export (📁): Save the current badge design to a **BDG** file so it can be imported to another system.

Cut (✂️): Delete the selected item on the badge template.

Copy (📄): Copy the selected item on the badge template.

Paste (📄): Paste the copied item onto the badge template.

Send to back (📄): Send the selected item to the background of the badge template. This option is helpful if you want to have a background image on the badge.

Bring to front (📄): Bring the selected item to the foreground of the badge template.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 320 of 430

3.11.6.4 Designing Badge Templates

To use customized printing templates for credential cards, you can design new badge templates that are tailored to your needs.

A badge template is represented by a **badge template entity** in *Security Center*, and can include fields from the configuration database so that the correct name, cardholder photo, and so on, will appear on each card.

For example, you can add a company logo, a background image, employee photo, or a custom color to be printed on the access control cards.

To design a badge template:

1. Open the **Access control** task, and click the **Badge template** view.
2. Click **Badge template** (+).
3. Type a name for the new badge template that appears in the entity list, and press **ENTER**.
4. In the **Identity** tab, type a description for the badge template.
5. In the **Relationships** section, select the partition where you want the badge template to be placed. **Partitions** determine which *Security Center* users have access to this entity. Only users who have been granted access to the partition can see the badge template.
6. Click **Apply**.
7. Click the **Badge designer** tab.
8. To select the size of the access control cards you want to print, click **Properties** (⚙️).
9. In the **Format** dialog box, select a card size and orientation.
 - To create custom card size, click (+), enter the card name, width, and length, and then click **OK**.
10. Click **OK**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 321 of 430

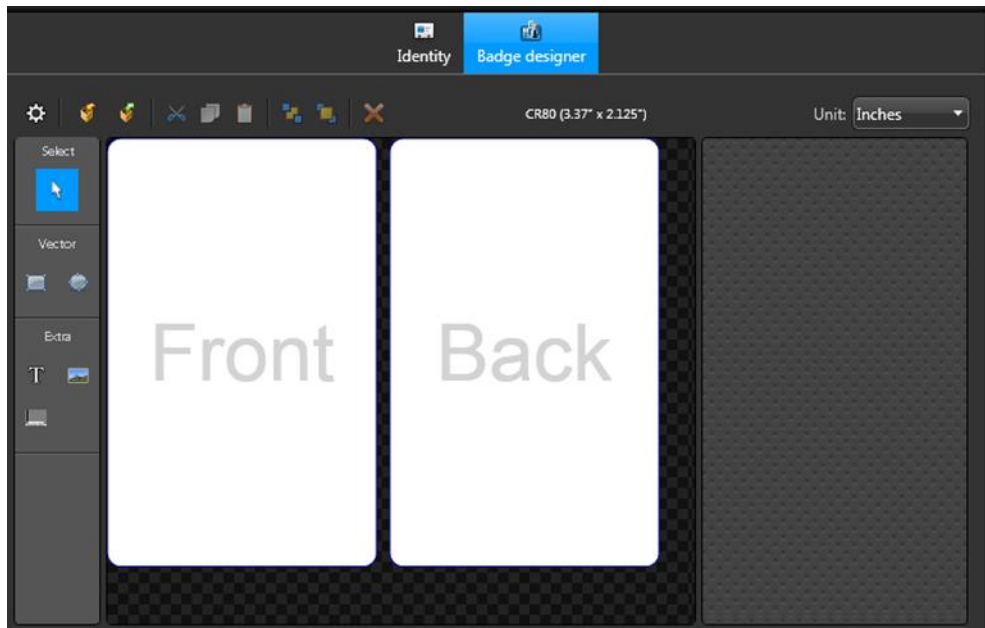


Figure 178. Badge Template: Badge Designer

Once the card size/format is chosen, you can design the actual printing template.

11. In the **Tools** section, select a tool, and then click on the template to use it.

There are six graphical tools you can use to edit the template:

- **Select tool:** Use to click and select an object on the template.
- **Rectangle tool:** Use to draw a square/rectangle on the template.
- **Ellipsis tool:** Use to draw circles/ovals on the template.
- **Text tool:** Use to insert text on to the template. You can enter a static text or add dynamic cardholder and credential text fields, such as *First name*, *Last name*, and so on.
- **Image tool:** Use to insert a picture on to the template. You can insert cardholder pictures, a background image for the card, and so on.
- **Barcode tool:** Use to insert barcodes on to the template.

12. If you added an image to the template, select the image to edit it using the options in the **Image** and **Color** and **border** widgets.

In the **Image** widget, choose whether the **Source** of the image is a *cardholder* picture or an image from a file, and whether the image should be stretched or not.

- **Cardholder's picture:** Dynamic cardholder picture that changes, depending on which cardholder credential you are printing. This image field links to the value **Cardholder picture** in the configuration database.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 322 of 430

TIP: If a cardholder's picture was taken in front of a *chroma* key screen, you can make the picture background transparent. This is helpful if you are creating a badge template that has an image in the background.

- **File:** Static image selected from a file.

In the **Color** and **border** widget, you can use the following tools:

- **Fill:** Use to modify the fill color of an inserted object like a square or oval.
- **Border:** Use to modify the border color of an inserted object.
- **Opacity:** Use to modify the opacity of an inserted object.
- **Border thickness:** Use to modify the thickness of the inserted object's border

13. If you added text to the template, select the text to edit it using the options in the **Text** widget.

Right-click the text field to select the **Z order**, the text **Border**, **Font**, **Color**, and **Alignment**.

In the **Text** widget, you can use the following tools:

- Click **Add field** (+) to add a dynamic cardholder or credential field. You can mix **static text** with the **dynamic** fields.
- Click **Fill** to set the text color.
- Click **Align left**, **center**, or **right** to set the text alignment.
- Click **Wrap text** if too long to turn on text wrapping.

If text wrapping is turned on, the system will wrap the text if it is too long to fit inside the text box, without changing the font size. If text wrapping is turned off, the system will fit the text inside the text box by changing the font size.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 323 of 430

14. If you added a barcode to the template, **right-click** the barcode, and then click **Properties** to edit it. The data on the barcode can be static or use dynamic credential properties.

Enter the text for the label:
{credentialname} +

Sample value:
123456789

☐ Include check digit
☒ Display barcode footer

Enter the barcode type:
Code 39

Narrow bar width in mil (1/1000 inch):
10.416

Wide bar width (factor of narrow bar width):
2

Quiet zone width (factor of narrow bar width):
10

Figure 179. Badge Template: Display Barcode Properties

15. In the **Size and position** section, select where the text, image, or barcode is located on the badge, and its width and height.
16. Click **Apply**.

Example

Here is a sample badge template with objects already inserted:



Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 324 of 430

Figure 180. Badge Template: Dynamic/Static Images

- Two different images have been inserted. One is dynamic, and the other is static:
 - The dynamic cardholder picture appears on the front of the card.
 - The static image appears on the back of the card. It is the company logo that is displayed on every card.
- Three dynamic text fields have been inserted:
 - **{Firstname} {lastname}** appears on the front of the card. The text printed will be taken from the configuration database and we will see first name, (space), last name. The text is centered and text wrapping is turned on.
 - **{Firstname} {lastname}** appears on the back of the card. This is the same as the name field on the front except with a smaller font size, and text wrapping is turned off.
 - **{Cardholder.Department}** Custom field that was created for the cardholder entity.
- A barcode has been inserted, containing dynamic data. It displays the credential name, using the barcode type **Code 39**.

3.11.6.5 Viewing Print Previews of Badge Templates

After you design a new badge template, you can see what it is going to look like on a credential card.

To view a print preview of a badge template:

1. Open the **Access control** task, and click the **Credentials** view.
2. Select the credential that you want to preview badge template with, and then click the **Badge templates** tab.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 325 of 430

3.12 ALARMS

An alarm is a type of entity that describes a particular trouble situation that requires immediate attention and how it can be handled in *Security Center*. For example, an alarm can indicate which entities (usually cameras and doors) best describe it, who must be notified, how it must be displayed to the user, and so on.

The basic properties of an alarm are:

- **Name:** Alarm name.
- **Priority:** Priority of the alarm (1-255), based on the urgency of the situation. Higher priority alarms are displayed first in Security Desk.
- **Recipients:** Users, user groups, and analog monitor groups who are notified when the alarm occurs and are responsible for responding to the alarm situation.
- **Broadcast mode:** How the alarm recipients are notified about the alarm.
- **All at once:** (Default) All recipients are notified at the same time, immediately after the alarm is triggered.
- **Sequential:** The recipients are notified individually, each after a specified delay (in seconds) calculated from the time the alarm is triggered. If the recipient is a user group, all members of the user group are notified at the same time.
- **Attached entities:** Entities that help describe the alarm situation (for example, cameras, area, doors, alarm procedure, and so on). When the alarm is received in *Security Desk*, the attached entities can be displayed one after another in a sequence or all at once in the canvas, to help you review the situation. If a composite entity is attached to the alarm, the entities that compose it are also attached to the alarm. For example, if a door entity is attached to the alarm, the cameras associated to the door are also attached to the alarm.

3.12.1 How Alarms Display in the Security Desk Canvas

You can view active and past alarms in the canvas in the **Alarm monitoring** task, the **Alarm report** task, and the **Monitoring** task.

In the **Alarm monitoring** task and **Monitoring** task, active alarms are automatically displayed in the canvas so you can review the alarm details and the associated video. In the **Alarm report** task, all videos associated to the alarm are displayed in playback mode. The playback starts at the time the alarm was triggered.

Alarms are often composite entities because they are attached to multiple cameras, doors, or areas, and might include still frames. To view all the attached entities at once, you must unpack the tile where the alarm is displayed.

- **NOTE:** If the triggered alarm is attached to an entity (for example a door) that is linked to cameras, then the linked cameras are displayed first in the canvas, before the attached entity itself.

[Figure 181](#) shows an active alarm in a canvas tile in the **Alarm monitoring** task.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 326 of 430



Figure 181. Alarm Management: Active Alarm in Canvas Tile

The following letters correspond to [Figure 181](#).

- A. Source of the alarm
- B. Alarm timestamp
- C. Allows you to view all attached entities at once
- D. On-tile video controls
- E. Timeline
- F. Alarm name
- G. Alarm instance number
- H. Displays the alarm procedure if it is defined

3.12.2 Enable Alarm Monitoring in the Monitoring Task

To avoid switching between tasks when an alarm occurs, you can enable alarm monitoring in the **Monitoring** task.

Once tiles are armed to monitor alarms in the Monitoring task, alarms longer appear as pop-ups in the notification tray. You can configure alarms as pop-ups.

To Enable Alarm Monitoring in the Monitoring Task:

1. Open the **Monitoring** task.
2. At the bottom of the **Monitoring** task, click **Monitoring** (🔍).
3. Switch the **Alarm monitoring** option to **ON**.
 - You can arm or disarm all the tiles from monitoring alarms by clicking (🔍). When a tile is armed to monitor alarms, the tile ID background is red.
4. Select whether you want to monitor **All alarms** or **Specific alarms**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 327 of 430

5. If you selected **Specific**, do the following:

- A. Click (+) and select the alarms you want to monitor.
 - **TIP:** To select multiple alarms, hold **CTRL** or **SHIFT** when selecting the alarms.
- B. Click **Add**.

The **Events** and **Alarms** toggle button appears in the top-right corner of the **Monitoring** task so you can easily switch between monitoring events and alarms. You can pause tile monitoring at any time by clicking **Suspend tile monitoring**.

3.12.3 Alarm Information Available When Monitoring Alarms

When an alarm is triggered, you can view the following information in the **Alarm monitoring** and the **Monitoring** task.

- **ID:** Alarm instance number. Uniquely identifies each alarm instance.
- **Alarm:** Alarm entity name.
- **Priority:** Alarm priority. All alarms imported from Omnicast have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.
- **Alarm color:** Color of the alarm.
- **Source:** The source entity that triggered the alarm, when the alarm is triggered by an event-to-action. It shows a username when the alarm is triggered manually.
- **Triggering event:** Event that triggered the alarm (if triggered through an event-to-action). Manual action is indicated when the alarm was manually triggered by a user.
- **Trigger time:** Time the alarm was triggered in Security Center.
- **State:** Current state of the alarm.
 - **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the **Report** pane.
 - **Acknowledged (Default):** Alarm was acknowledged using the default mode.
 - **Acknowledged (Alternate):** Alarm was acknowledged using the alternate mode.
 - **Acknowledged (Forcibly):** Alarm was forced to be acknowledged by an administrator.
 - **Under investigation:** Alarm that is under investigation, meaning that someone has seen it but not necessarily able to take care of it.
 - (5.6 and earlier) Alarm under investigation with an acknowledgement condition that is still active. These alarms cannot be acknowledged until the condition is cleared.
 - **Acknowledgement required:** Alarm with an acknowledgement condition that was cleared and that is ready to be acknowledged.
- **Context:** Alarm annotation.
- **Acknowledged by:** User who acknowledged the alarm. When the alarm is acknowledge automatically by the system, Service is indicated.
- **Acknowledged on:** Time the alarm was acknowledged.
- **Investigated by:** The user who put the alarm into the under investigation state.
- **Investigated on:** The timestamp when the alarm was put into the investigation state.
- **Occurrence period:** Period when the event occurred.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 328 of 430

- **Source entity type:** The source entity type that triggered the alarm, when the alarm is triggered by an event-to-action. It shows User when the alarm is triggered manually.
- **Source time:** Time of the alarm-triggering event. The only time Source time and Triggering time are different is when the event occurred while the access control unit was offline.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.

3.12.4 Mute Repeated Alarm Sounds

If many active alarms on your system are causing sound bites to be repeatedly played, you can silence the alarm sounds by muting them from the **Notification** tray.

To avoid unintentionally ignoring alarms, you can configure your *Security Desk* to play a sound bite repeatedly as long as there are active alarms in the system. The sound will stop when all alarms are acknowledged, or when you decide to mute them temporarily.

To mute all sounding alarms:

1. In the **notification** tray, right-click the **Alarms** icon , and click **Mute** all alarms.
2. All sounding alarms are muted. The sounding will restart the moment a new alarm is received and will continue as long as there are active alarms in the system.

3.12.5 Forward Alarms to Other Users Automatically

If you must leave your desk and you want someone else to receive alarms while you are gone, you can set alarms to auto-forward. Make sure that you have the Forward alarms user privilege.

To forward an alarm automatically:

1. Do one of the following:
 - In the notification tray, right-click the **Alarms** icon  or  and click **Start alarms auto-forward**.
 - In the upper-left corner of the **Alarm monitoring** or **Monitoring task**, click **Start alarms auto-forward** .
2. In the **Select alarm recipients** dialog box, select the destination user or user group.
3. Optional: Write a message to send with the forwarded alarm.
4. Click **Start alarms auto-forward**. All alarms sent to you are forwarded to the specified user until you cancel the auto-forward option.
5. To cancel auto-forward, do one of the following:
 - In the notification tray, right-click the **Alarms** icon  or  and click **Stop alarms auto-forward**.
 - In the upper-left corner of the **Alarm monitoring** or **Monitoring task**, click **Stop alarms auto-forward** .

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 329 of 430

3.12.6 Forward Alarms to Other Users Manually

If you receive an important alarm and you want someone else to see it, you can manually forward the alarm to them from the **Alarm monitoring**, **Monitoring**, and **Alarm report** tasks.

Make sure that you have the **Forward alarms** user privilege.

Forwarding an alarm does not remove it from your workspace. The alarm is forwarded to the user you selected, and one of you must acknowledge the alarm.

To Forward an Alarm Manually:

1. Under the alarm list, or in the alarm widget, click **Forward** alarm (🔄).
2. In the **Select alarm recipients** dialog box, select the destination user or user group.
3. (Optional) Write a message to send with the forwarded alarm.
4. Click **Forward alarm**.

3.12.7 Alarm Priority

In *Security Desk*, alarms are displayed in the **Alarm monitoring** task and the **Monitoring** task by order of priority (this is evaluated every time a new alarm is received). The highest priority alarm is displayed in tile #1, followed by the second highest in tile #2, and so on. When two alarms have the same priority value, priority is given to the newest one.

When a new alarm is received in *Security Desk* with a priority level identical or higher than the current alarms displayed, it pushes the other alarms down the tile list.

When an alarm is acknowledged in *Security Desk*, it frees a tile for lower priority alarms to move up.

3.12.8 Video Recording on Alarms

When an alarm is triggered that has cameras attached to it, you can make sure that the video related to the alarm is recorded and available for future alarm investigations. The amount of time that the video is recorded for (called the guaranteed recording span) is defined by two settings:

- **The alarm recording duration:** Number of seconds that the **Archiver** records video for after the alarm is triggered. This option (Automatic video recording) is set in the alarm Advanced tab.
- **The recording buffer:** Number of seconds that the **Archiver** records video for before the alarm was triggered, to make sure that whatever triggered the alarm is also recorded. This option (Time to record before an event) is set in the **Archiver** Camera default settings tab, or for each camera individually.

If an alarm is triggered from a camera event (for example Object removed), then the camera that caused the event is also attached to the alarm and starts recording.

- **IMPORTANT:** The recordings are dependent on the archiving schedules. If recording is disabled when the alarm is triggered, no video is recorded.

3.12.9 Select Video Display Options for Alarms

If a camera is attached to an alarm, you must configure how the video is shown when the alarm is triggered and displayed in the canvas of the **Alarm monitoring** task. The default video display option is live video. You can select live video, playback video, a series of still frames before, during, or after the alarm is triggered, or a combination of the three. The video or still frames are displayed

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 330 of 430

for the number of seconds set in the **Content cycling** option in the alarm **Properties** tab. The options you set are applied to all cameras that are attached to the alarm.

To select the video display options for an alarm:

1. Open the **Alarms** task and click the **Alarms** view.
2. Select the alarm to configure, and click the **Properties** tab.
3. From the **Video display** option drop-down list, select one of the following:
 - **Live**: Display live video.
 - **Playback**: Display playback video.
 - **Live and playback**: Cycle between displaying live and playback video. When you unpack the tile, one tile displays live video and the other displays playback. You can also click the **Properties** icon (⚙️) and configure **Picture-in-picture** so you can view the live and playback video in the same tile.
 - **Live and still frames**: Cycle between displaying live video and a series of still frames. When you unpack the tile, one tile displays live video and the other displays still frames. You can also click the **Properties** icon (⚙️) and configure **Picture-in-picture** so you can view the live and still frames video in the same tile.
 - **NOTE**: Still frames are not supported when the camera is encrypted.
 - **Still frames**: Display a series of still frames. See previous note.
4. If you select a display option that includes playback video, then select how many seconds before the alarm was triggered to start the playback.
 - **NOTE**: To ensure that playback video is available for the length of time you set, the recording buffer for events must be an equal or larger value.
5. If you select a display option that includes still frames, click the **Properties** icon (⚙️).
6. In the **Still frames** dialog box, select whether you want each still frame to be displayed for the same duration or an independent duration of time (Same durations or Independent durations).
7. If you select **Same durations**, then set the following options:
 - **Number of frames**: Select the number of still frames to display within total content cycling duration.
 - **Play**: Select how many seconds before the alarm was triggered to start the first still frame.
8. If you select Independent durations, do the following:
 - A. Click **Add an item** (+).
 - B. In the **Relative time** option, select how many seconds before or after the alarm was triggered the still frame displays.
 - C. In the **Duration** option, select how long the still frame is displayed for.
 - D. Click **Add**.
 - E. Add additional still frames.

The duration of all the still frames cannot exceed the **Total duration** value.
9. If you select the **Live and Playback** or **Live and still frames** option, you can configure picture-in-picture to display both live and playback video or live and still frame video in the same tile.
 - A. Click the **Properties** icon (⚙️).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 331 of 430

- B. In the **Video display configuration** dialog box, from the **Picture-in-picture** list, choose what type of video you would like to be displayed in the inset window.
 - C. From the **Displayed at** list, select where you would like the inset window to be displayed.
5. Click **OK > Apply**.

3.12.10 Setting Optional Alarm Properties

After you create an alarm and configure its basic properties, there are additional properties you can set.

To set optional properties for an alarm:

1. Open the **Alarms** task and click the **Alarms** view.
2. Select the alarm to configure, and click the **Advanced** tab.
3. Set the following options:
 - **Reactivation threshold:** The minimum time *Security Center* needs to wait after triggering this alarm before it can be triggered again. This option prevents the system from repeatedly triggering the same alarm before it is resolved.
 - **Alarm procedure (URL):** Enter the URL or the web page address corresponding to the alarm procedure, which provides alarm handling instructions to the operators. The web page is displayed when the user clicks **Show alarm procedure** (📄) in the alarm widget in *Security Desk*.
 - **Schedule:** Define when this alarm is in operation. Outside the periods defined by this schedule, triggering this alarm has no effect.
 - **NOTE:** You can add multiple schedules to the alarm. Schedule conflicts that cannot be resolved will be notified.
 - **Automatic acknowledgment:** Turn this option on to let the system automatically acknowledge this alarm if no one acknowledges it before the specified time (in seconds). This option is recommended for low-priority alarms that serve to alert the security operator, but do not require any action. When this option is turned off, the system follows the **Auto ack alarms after** option configured at the system level in **Server Admin**.
 - **NOTE:** Automatic acknowledgement does not apply to alarms that have an active condition attached. To acknowledge those alarms, you need to forcibly acknowledge them (which requires the Forcibly acknowledge alarms privilege). For more information on acknowledging alarms, see the *Security Desk User Guide*.
 - **Create an incident on acknowledgement:** Turn this option on to prompt the *Security Desk* user to report an incident every time they acknowledge an alarm.
 - **NOTE:** Turning this option on turns the automatic acknowledgement option off.
 - **Automatic video recording:** Turn this option off (default=on) if you do not want to start recording video when the alarm is triggered.
 - **Protect recorded video:** Turn this option on (default=off) to protect the video recordings associated to this alarm for the specified number of days.
 - **Alarm sound:** Select the sound bite to play when a new alarm occurs, if alarms are configured to play a sound in *Security Desk*. By default, the sound bite that is configured in the **Security Desk Options** dialog box is used.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 332 of 430

- **Color:** Select a color for the alarm. The color is used for the overlay of the alarm video when it is displayed in a tile in the Alarm monitoring or Monitoring task, as well as when the alarm is triggered on a map.

4. Click **Apply**.

3.12.11 Troubleshoot Alarms not Received

If you do not receive an alarm in Security Desk, you can troubleshoot the cause of the issue.

To Troubleshoot Why an Alarm is not Received:

1. Make sure the user who is trying to receive the alarm is a recipient of the alarm, as follows:
 - A. Open the **Alarms** task and click the **Alarms** view.
 - B. Select the alarm, and click the **Properties** tab.
 - C. Make sure the user, or the user group they are a member of, is in the **Recipients** list.
2. Make sure the alarm schedule is not preventing you from triggering the alarm at this moment, as follows:
 - A. Click the **Advanced** tab of the alarm.
 - B. Make sure the schedule listed in the **Schedule** drop-down list applies at this time.
3. Make sure the alarm recipient has the correct user privileges to receive alarms, as follows:
 - A. From the **Config Tool** home page, open the **User management** task.
 - B. Select the user to configure, and click the **Privileges** tab.
 - C. Make sure the **Alarm monitoring** and **Acknowledge alarms user privileges** are set to **Allow**.
 - D. Click **Apply**.

3.12.12 Set Up Alarms Using Event-to-Actions

You can configure alarms so that they are triggered when an event occurs, using event-to-actions.

To Set up an Alarm Using an Event-to-Action:

1. Open the **System** task and click the **General settings** view.
2. Click the **Actions** tab and click (+).
3. In the **Entity** type page, select an entity type, and click **Next**. The source entity is the entity that the event is attached to.
4. In the **Source** page, select the source entity and click **Next**.
5. In the **Event** page, select an event type. Only events related to the selected entity type are listed.
6. Select a schedule and click **Next**.

The schedule determines when the event will trigger the action. For example, you might want to trigger an alarm only if a window is opened during the weekend. By default, **Always** is selected.

7. In the **Action** page, select **Trigger alarm**.
8. From the **Alarm** drop-down list, select an alarm to trigger.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 333 of 430

9. (Optional) From the **Acknowledgement** condition drop-down list, select an event that must be triggered before the alarm can be acknowledged.

This option is only available for some event types.

10. To require a user to acknowledge the alarm after the acknowledgement condition is cleared, select the **User acknowledgement required** option. If you clear this option, the alarm is automatically acknowledged when the **acknowledgement** condition is cleared.
11. Click **Next** > **Create** > **Close**.

3.12.13 Event Types That Can Require Acknowledgement Conditions

Some event-to-actions can be configured so that a second event must be triggered before the alarm that was triggered can be acknowledged. The second event is the acknowledgement condition.

For example, you can configure a Signal lost event to trigger an alarm and specify that the alarm can only be acknowledged after the Signal recovered event is generated.

[Table 37](#) lists the event types that gives you the option to configure an acknowledgement condition that must be cleared before the alarm can be acknowledged.

Table 37. Event Acknowledgement Conditions

Source Event Type	Entity Type	Acknowledgement Condition
AC fail	Access control unit, Intrusion detection unit	AC ready
Application lost	Roles	Application online
Asset offline	Asset	Asset online
Asset online	Asset	Asset offline
Battery fail	Access control unit, Intrusion detection unit	Battery ready
Door closed	Door	Door closed
Door forced open	Door	Door closed Input Normal Input Active
Door opened	Door	Door closed Input Normal Input Active
Door open too long	Door	Door closed
Hardware tamper	Access control unit, Intrusion detection unit, Zone (hardware)	Tamper normal
Intrusion detection area alarm activated	Intrusion detection area	Disarmed (not ready) Disarmed (ready to arm) Master armed Perimeter armed
Intrusion detection area input bypass activated	Intrusion detection area	Input normal

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 334 of 430

Source Event Type	Entity Type	Acknowledgement Condition
Intrusion detection unit tamper	Intrusion detection unit	Tamper normal
Manual station activated	Door	Manual station normal - Input Normal - Input Active
Recording problem	Camera	Recording problem resolved (corresponds to <i>Recording on</i> or <i>Recording off</i>)
Signal lost	Camera	Signal recovered
Unit lost	Access control unit, Intrusion detection unit, LPR unit, Video unit	Unit online
Zone armed / Zone disarmed ¹	Zone	- Zone state normal - Zone state active
¹ Events that are associated with the normal, active, and trouble states of a zone can also be configured with an acknowledgement condition.		

3.12.14 Alarm Acknowledgement Conditions

- A. Alarm is triggered and sent to user.
- B. User validates alarm, and then clicks.
Acknowledge to dismiss the alarm.

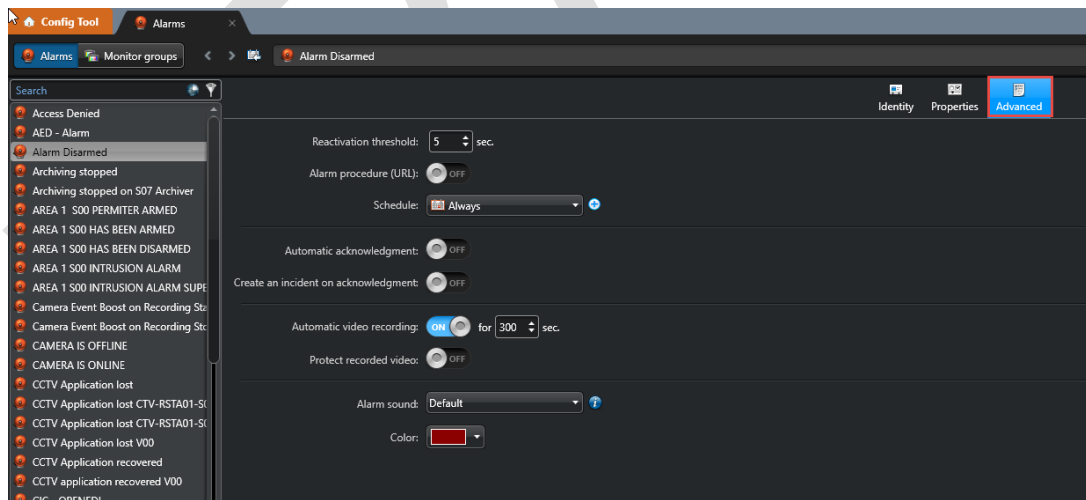


Figure 182. Alarm Management: Alarm Acknowledgement Conditions

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 335 of 430

3.12.15 Acknowledging Alarms

You can view and acknowledge the alarms from the **Alarm monitoring** and the **Monitoring** task. To view and acknowledge alarms from the **Monitoring task**, you must enable alarm monitoring for that Monitoring task.

You only receive an alarm in *Security Desk* if you are a recipient of that alarm. Alarms are displayed in the canvas by order of their priority.

NOTE: You might not have to acknowledge all the alarms that are triggered. Certain alarms are configured to be automatically acknowledged after a set amount of time.

To acknowledge an alarm:

- In the notification tray, double-click the **Alarms** () icon in the notification tray.
All new alarms are automatically listed, and the associated video is displayed in the canvas.
- To filter the alarm list, click the **filter** icon () and select one or more of the following filters:
 - Show all:** Display all alarms (no filter).
 - Show active:** Show active alarms.
 - Show under investigation:** Show alarms that are currently under investigation.
 - Show acknowledgement required:** Show alarms where their source conditions are cleared but they must still be acknowledged.
 - Show acknowledged:** Show acknowledged alarms.
- Double-click or drag an alarm from the alarm list to view the alarm video in a tile. The video is displayed with a colored overlay that provides the alarm details.
- Click one of the following:
 - Acknowledge** (Default) (): Acknowledge the alarm. The alarm is no longer active, and is removed from the canvas and the alarm list.
 - NOTE:** Certain alarms require you to report an incident when you acknowledge them.
 - Acknowledge** (Alternate) (): Set the alarm to the alternate acknowledged state. The reasons for using this acknowledgement type are defined by your company. For example, if a false alarm is triggered, you can acknowledge the alarm this way. This state can be used as a filter in alarm queries.
 - Investigate** (): Investigate the alarm. This action lets other users in the system know that you have seen the alarm without acknowledging it, so the alarm is not removed from the active alarm list.
 - NOTE:** For 5.6 and earlier, this button is only available if the alarm has an acknowledgement condition attached, and the condition is not yet cleared.
 - Forcibly acknowledge** (): Force the alarm to be acknowledged. This is helpful for clearing alarms that are currently under investigation and their acknowledgement condition is not yet cleared.
 - Forcibly acknowledge all alarms** (): Force all the active alarms to be acknowledged. This is helpful for clearing alarms that are currently under investigation and their acknowledgement condition is not yet cleared.
 - Snooze alarm** (): Put the alarm to sleep for 30 seconds. When the alarm is snoozing, it is temporarily removed from the canvas. You can change the default snooze time from the **Options** dialog box.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 336 of 430

- **Show alarm procedure** (📄): Show the alarm's specific procedure (if one is defined by the administrator). Alarm procedures are simple to create and can take the form of HTML pages or a web application developed by the end user.
- **Forward alarm** (➡): Forward the alarm to another user in the system. Before forwarding the alarm, you must select a user, and you can also type a message.
- **Edit context** (✎) Add or modify the alarm annotation.
- **NOTE:** All actions on the alarms are logged in the activity trail.

3.12.16 Clear Source Condition

Alarms can be configured such that user acknowledgement is not possible until the source condition that triggered the alarm has been cleared.

Table 38. Alarm Management: Clear Source Condition

Alarm Trigger	Acknowledgment Not Possible	Acknowledgement Available
Door held open	As long as the door hasn't closed	Once the door has closed
Camera offline	As long as the camera is still offline	Once the camera has come back online

3.12.17 Incident Report Requirement

Alarms can be configured such that user acknowledgment is not possible unless the user creates an incident report.

Report an incident (Alarm #4)

Title: False alarm #2

Category: False alarm

Description: Another false alarm due to the faulty cabling.

References

- Fire escape

Incident time: 4/3/2015 5:44:45 PM

Cancel Create

Figure 183. Alarm Management: Report an Incident

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 337 of 430

3.12.18 Receiving Alarms

Default: Alarm monitoring task opens automatically in the recipient's *Security Desk*.

In [Figure 184](#), the same alarm shown graphically in a tile. Alarm shown in text mode in the alarm list.

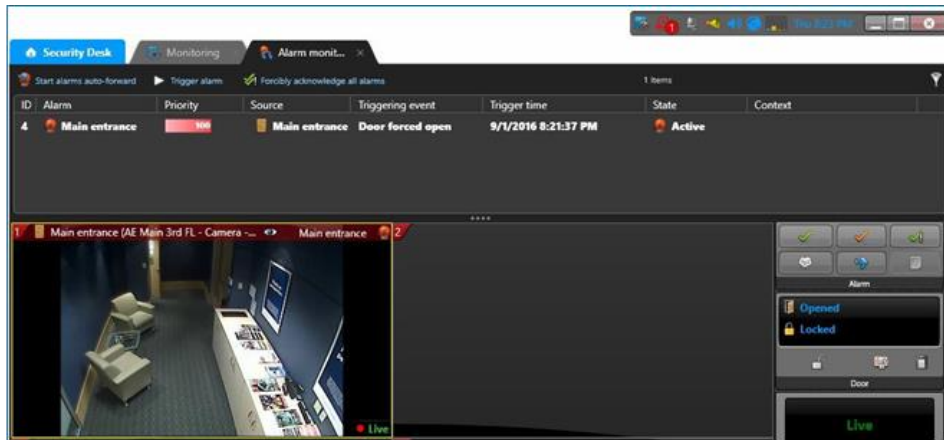


Figure 184. Alarm Management: Alarm Monitoring

3.12.19 Alternative Display Mode

For an alternate display of alarms:

1. Go to **Security Desk Home** page
2. Select **Options**
3. Select **Alarms**
4. In the **Display In** section, select one of the radio buttons for your display options.

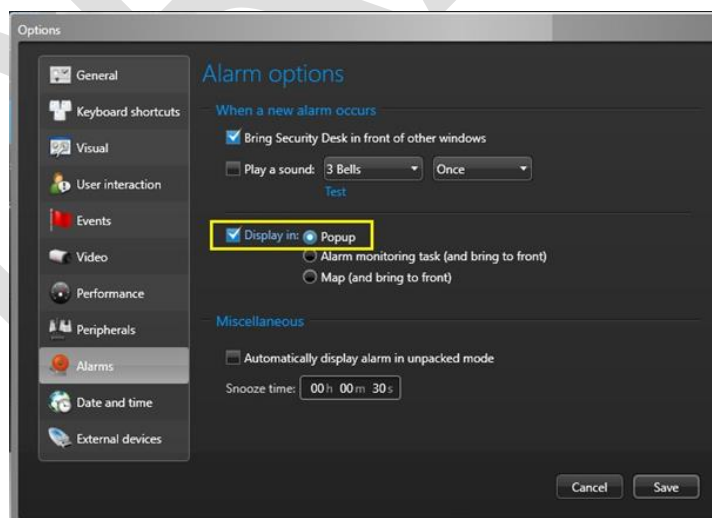


Figure 185. Alarm Management: Alarm Options

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 338 of 430

3.12.20 Popup Alarm Display

Alarm is shown from the notification tray of the *Security Desk*.

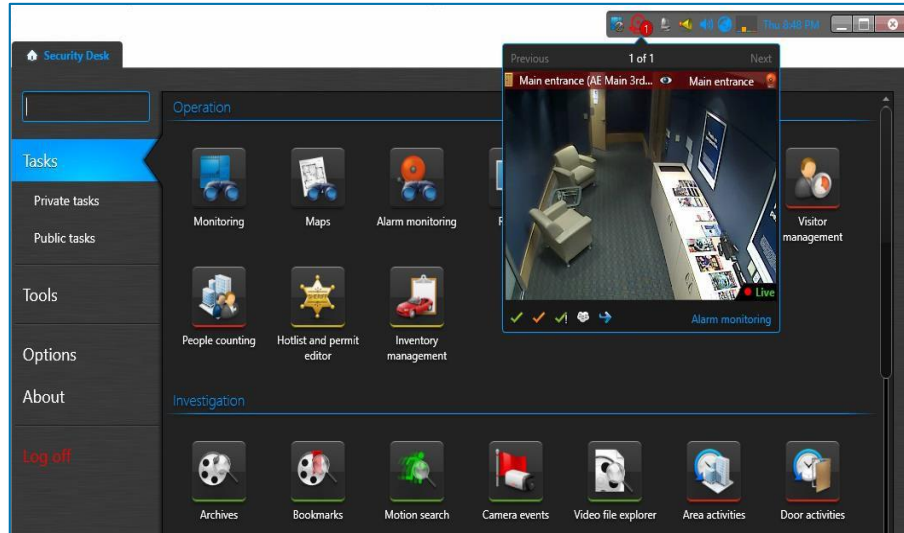


Figure 186. Alarm Management: Popup Alarm Display

3.12.21 Grouping Alarms

Monitoring and **Alarm Monitoring** tasks: can now group alarms for easier management and visibility.

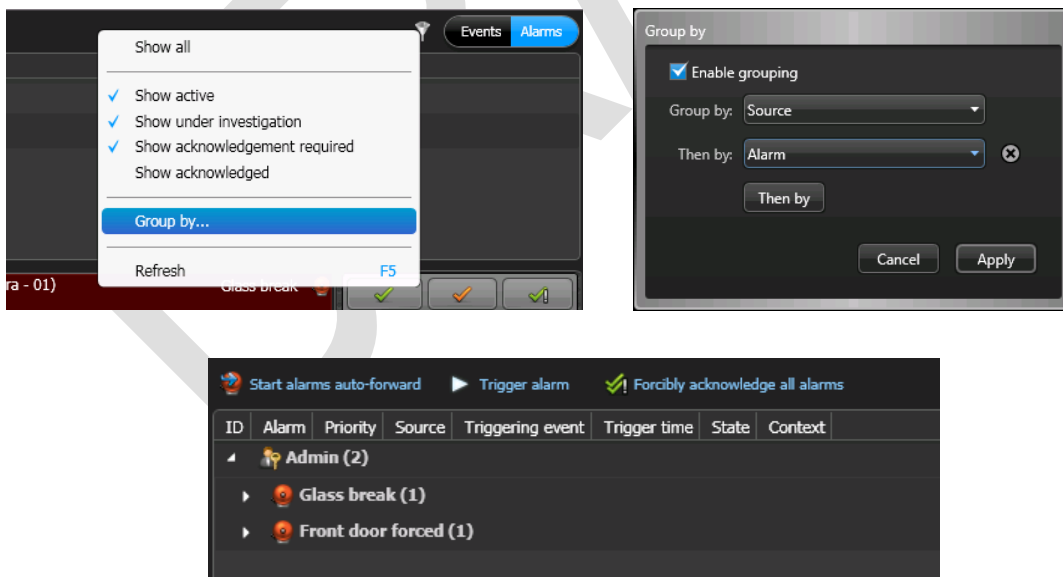


Figure 187. Alarm Management: Grouping Alarm

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 339 of 430	

3.12.21.1 Filter and Group Alarms in Security Center

You can filter and group alarms to control how they appear in the Alarm monitoring task and the **Monitoring** task.

To filter alarms:

1. In the **Alarm monitoring** task or the **Monitoring** task, click the **filter** icon ().

NOTE: In the **Monitoring** task, you must select **Alarms** from the **Events/Alarms** toggle button. The **Events/Alarms** toggle button only appears when you enable alarm monitoring in the **Monitoring** task.

If you cannot see the **Filter** () or **Events/Alarms** toggle button, drag the top of the canvas down to expose the alarm list that appears at the top of the screen.

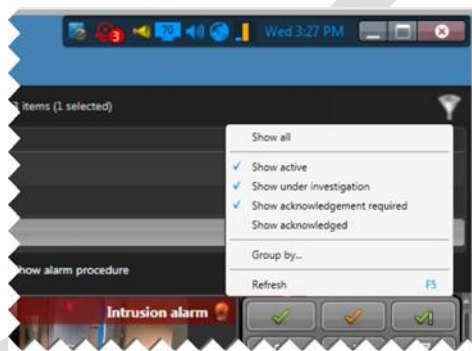


Figure 188. Alarm Filters

2. Select or clear the following filters:
 - **Show all:** Display all alarms (no filter).
 - **Show active:** Show active alarms.
 - **Show under investigation:** Show alarms that are currently under investigation.
 - **Show acknowledgement required:** Show alarms where their source conditions are cleared but they must still be acknowledged.
 - **Show acknowledged:** Show acknowledged alarms.

To group alarms:

1. In the **Alarm monitoring** task or the **Monitoring** task, right-click a column heading and select **Group by**.

NOTE: In the **Monitoring** task, you must select **Alarms** from the **Events/Alarms** toggle button. The **Events/Alarms** toggle button only appears when you enable alarm monitoring in the **Monitoring** task. If you cannot see the **Events/Alarms** button, drag the top of the canvas down to expose the alarm list that appears at the top of the screen.
2. In the **Group by** dialog box, select **Enable grouping**.
3. From the drop-down list, select the highest level of grouping you would like to apply to the alarms.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 340 of 430

You can group the alarms by:

- **Alarm:** Alarm entity name.
 - **Priority:** Alarm priority. All alarms imported from Omnicast have their priority set to 1 by default. You can change their priority at a later time in the **Config Tool**.
 - **Source:** The source entity that triggered the alarm, when the alarm is triggered by an event-to-action. It shows a username when the alarm is triggered manually.
 - **Source entity type:** The source entity type that triggered the alarm, when the alarm is triggered by an event-to-action. It shows User when the alarm is triggered manually.
 - **State:** Current state of the alarm:
 - **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the **Report** pane.
 - **Acknowledged (Default):** Alarm was acknowledged using the default mode.
 - **Acknowledged (Alternate):** Alarm was acknowledged using the alternate mode.
 - **Acknowledged (Forcibly):** Alarm was forced to be acknowledged by an administrator.
 - **Under investigation:** Alarm that is under investigation, meaning that someone has seen it but not necessarily able to take care of it.
 - (5.6 and earlier) Alarm under investigation with an acknowledgement condition that is still active. These alarms cannot be acknowledged until the condition is cleared.
 - **Acknowledgement required:** Alarm with an acknowledgement condition that was cleared and that is ready to be acknowledged.
4. To apply additional grouping levels, select **Then by**.
 5. Click **Advanced**.
 6. To change the grouping order, select a group, and then use the (↕) and (↕) arrows.
 7. To show alarm information in the header of the group, perform the following steps:
 - A. Select a group, and then click **Edit the item** (✎).
 - B. Select the alarm columns you want to show.
 - C. To change the column order of appearance, use the (↕) and (↕) arrows.
 - D. Click **OK**.
 8. Click **Apply**.

3.12.22 Server Alarm Trigger

The ICCS defines automatic actions triggered by alarms; refer to the ICCS database controlled through the ICCS server. [Figure 189](#). ICCS Generic Alarm Command shows generic command triggered by alarms.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 341 of 430

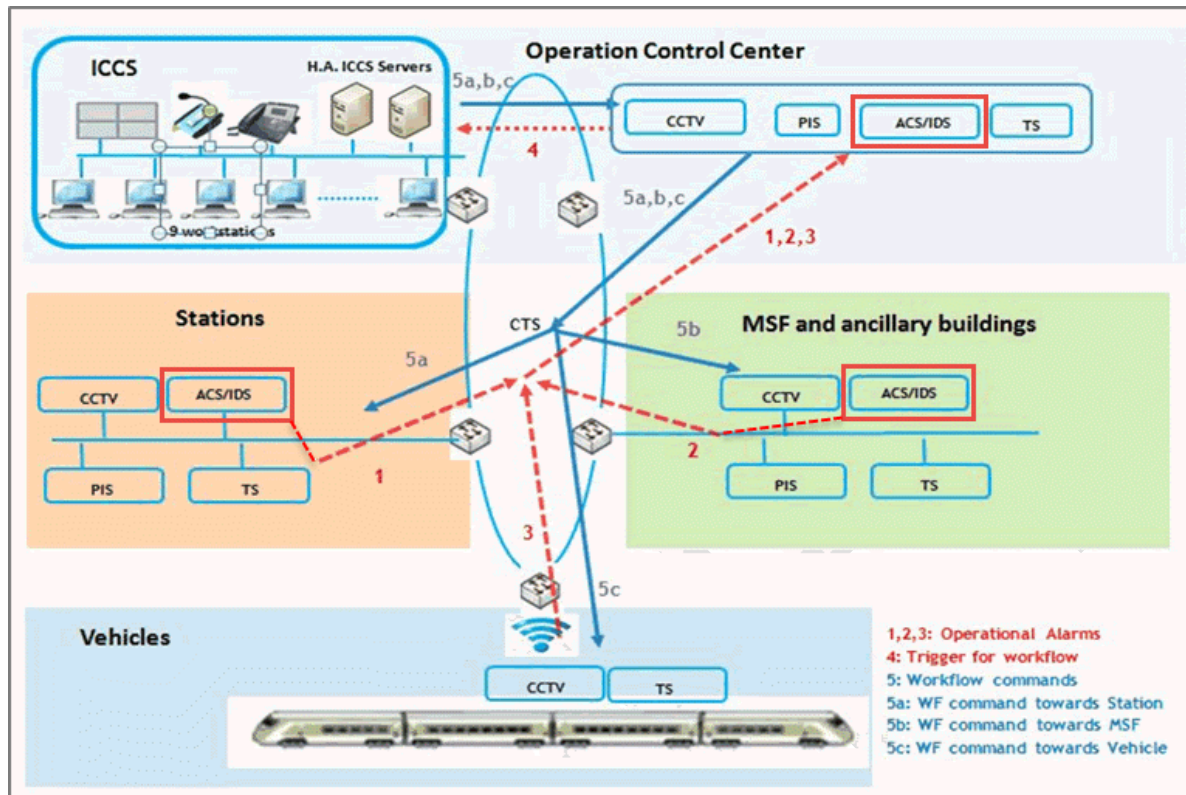


Figure 189. ICCS Generic Alarm Command

3.12.22.1 Alarm Trigger Example

One example of a possible use case supported by the ICCS illustrates a workflow when an intrusion or unauthorized access is detected at a restricted zone. Stages of this scenario would be as follows:

1. Intrusion is detected or entry access is denied to a person in a restricted zone.
2. An access control or intrusion detection device is deployed in this zone and is managed remotely by the ACS or IDS subsystem on the ICCS.
3. An alarm is raised in the **ICCS Alarm Manager** against the **ACS** or **IDS** subsystem
4. If the critical alarm defined in the **ICCS** condition rule is raised and appears in the **ICCS Alarm Manager**, the following commands are predefined:
 - Identify the CCTV camera device nearest to the location of the ACS or IDS and automatically play the live camera image of the restricted zone in the CCTV video wall
 - Pan, tilt, and zoom the CCTV camera device to the restricted zone
 - Set a bookmark of the timeline in the CCTV subsystem recorder
5. Operator's manual actions: authorize or deny access to the restricted zone after viewing the CCTV footage or discussing with field personnel
 - **Post-condition rule:** The critical alarm raised in the **ACS** or **IDS** subsystem is closed.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 342 of 430	

- **Post-condition rule commands:** If a post-condition rule is defined for closure of a critical alarm in the **ICCS Alarm Manager**, the following workflow actions are predefined:
 - Move the CCTV camera device to the initial position and remove the video stream from the video wall.

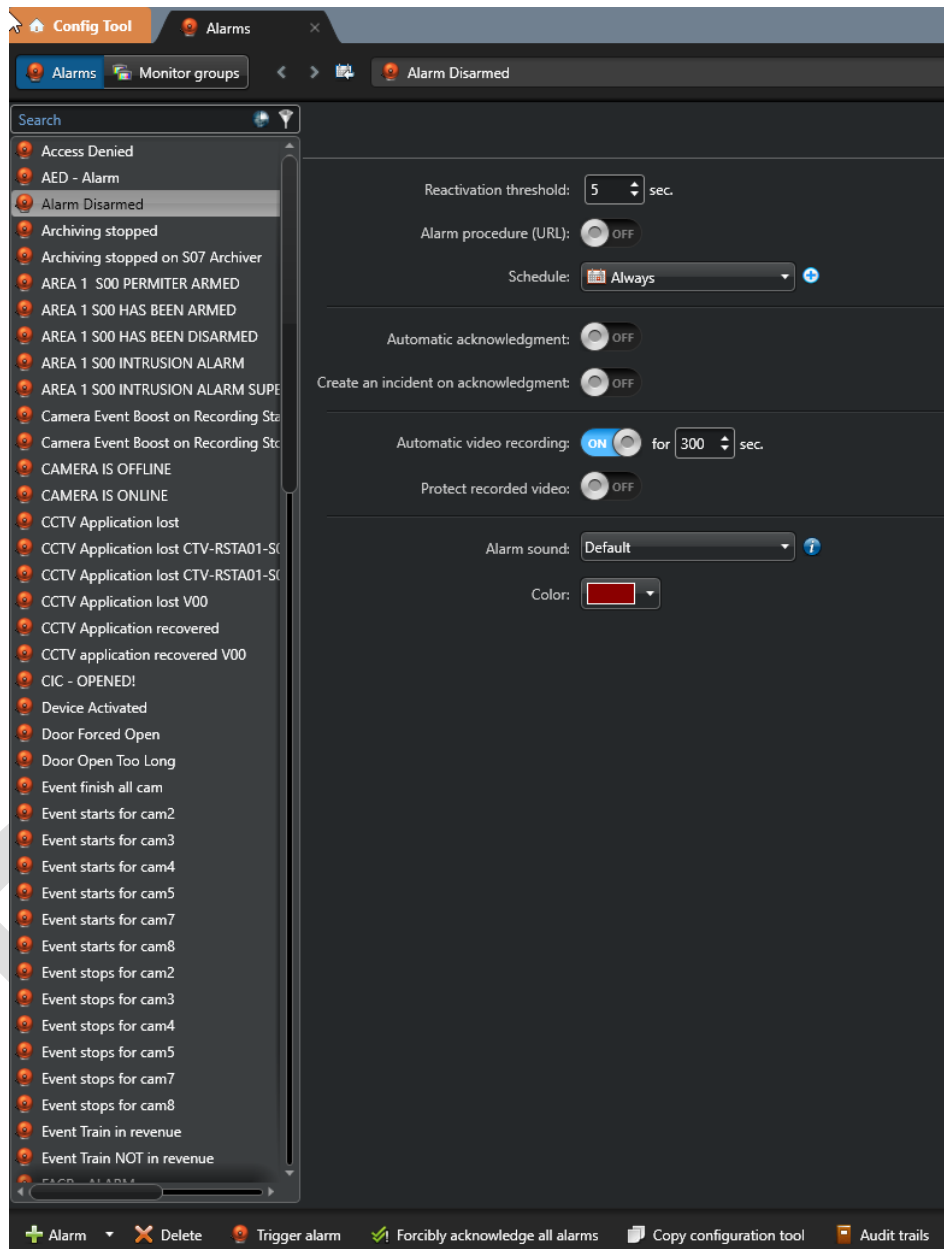


Figure 190. Alarm Management: Monitor Alarm Groups

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 343 of 430	

3.12.23 Trigger an Alarm

Alarms are usually triggered manually for testing purposes.

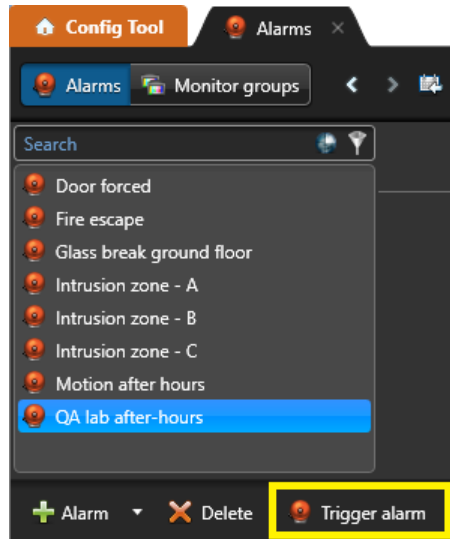


Figure 191. Alarm Management: Trigger Alarm

Once deployed, alarms are usually triggered with *Security Center's* event handling mechanism.

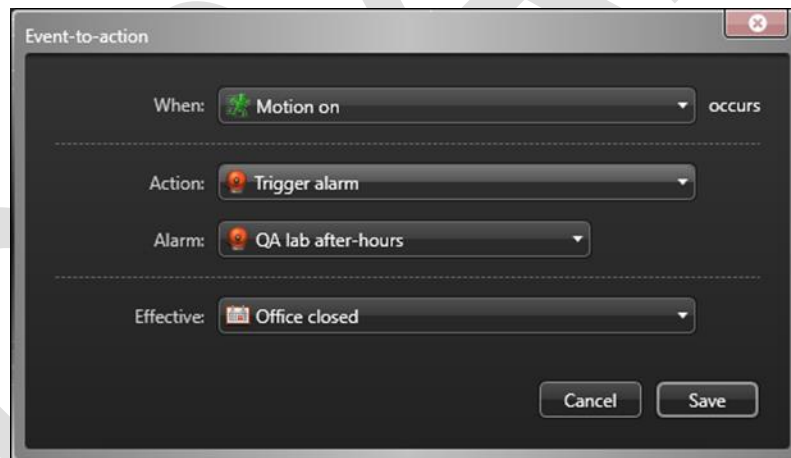


Figure 192. Alarm Management: Event to Action

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 344 of 430

3.12.23.1 Trigger Alarms Manually

To test an alarm that you just created, or if something critical occurs and you want to activate an alarm, you can trigger the alarm manually.

Before you begin

- The alarm must be configured in **Config Tool**.
- If you want to trigger alarms from the **Monitoring** task, you must enable alarm monitoring.

To Trigger an Alarm Manually:

- Do one of the following:
 - In the **Config Tool Alarms** task, select an alarm, and then click **Trigger alarm** (🔔) in the toolbar at the bottom of the workspace.
 - In the **Security Desk notification** tray, click Hot actions (🔔) > Manual action. Click **Trigger alarm** (🔔), select an alarm, and then click **OK**.
 - In the **Security Desk Alarm monitoring** task or Monitoring task, click **Trigger alarm** (▶), select an alarm, and click **Trigger alarm**.

All pre-configured alarm recipients receive the alarm if they are logged on to *Security Desk*.

3.12.24 Alarm Options

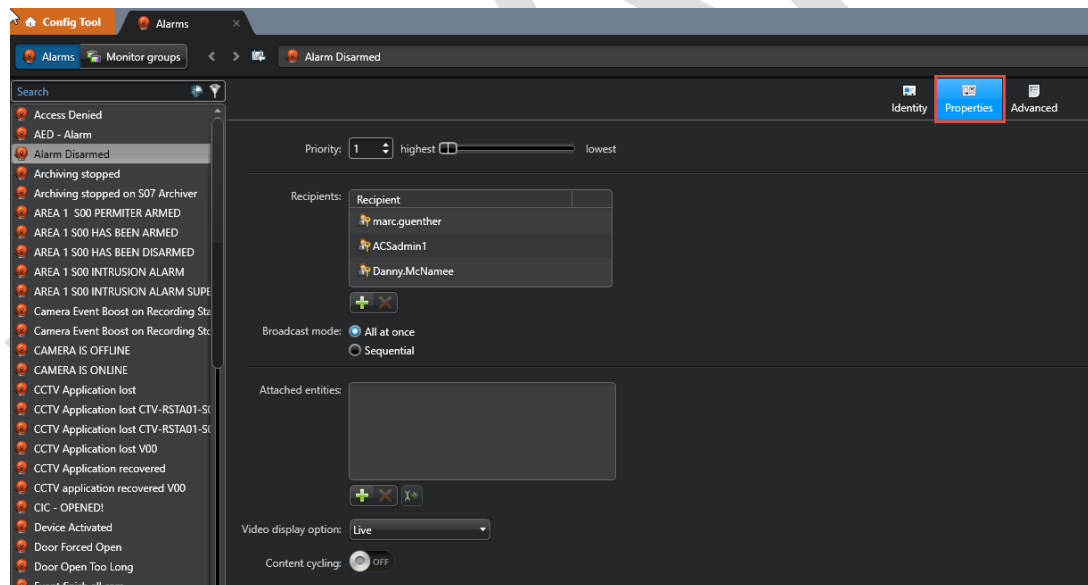


Figure 193. Alarm Management: Alarm Options

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 345 of 430

As indicated in [Figure 194](#) there are several options available to indicate when a new alarm occurs.

- You can bring the alarm window to the front of all other windows that are open
- Play a sound
- Display the alarm in a popup window or on a map, etc.

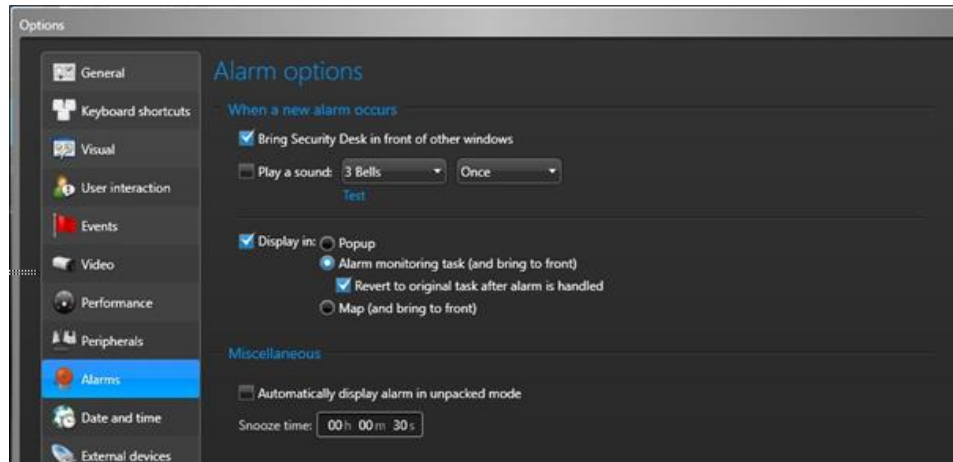


Figure 194. Alarm Management: Alarm Options

3.12.25 Alarm Privileges

Users must have the privilege to use the **Alarm monitoring** task and the privilege to acknowledge alarms if they are alarm recipients.

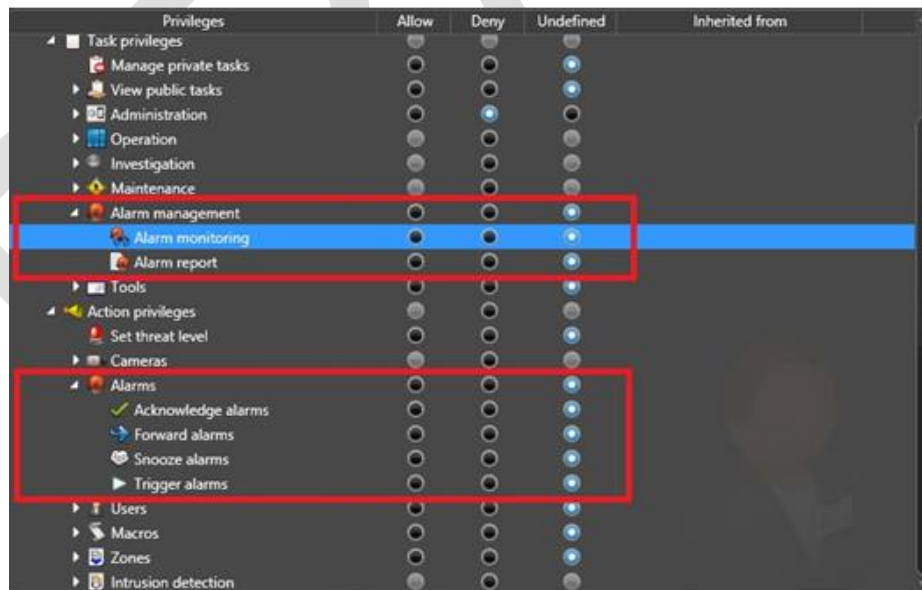


Figure 195. Alarm Management: Alarm Privileges

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 346 of 430

3.12.26 Customize Alarm Behavior

Once you are familiar with how alarms work, you can customize how the system handles alarms from the **Options** dialog box.

The **Display entity names** with their full path option is saved as part of your user profile. The other alarm settings are saved locally for your Windows user profile.

To Customize the Alarm Behavior:

1. From the home page, click **Options > Alarms**.
2. Set the following alarm options:
 - **Bring Security Desk in front of other windows:** Brings the *Security Desk* window to the foreground when a new alarm occurs.
 - **Play a sound:** Sets the sound bite to play when a new alarm occurs and how often to play it: Once (default), Every n seconds, or Continuously. Click **Test** to hear the selected sound bite.
 - **Display in:**
 - **Popup:** Select this option to have alarms appear in a popup window in the notification tray of the **Monitoring** task.
NOTE: Popup alarms only appear when there are no armed tiles in the **Monitoring** task.
 - **Alarm monitoring task (and bring to front):** Automatically switches to the **Alarm monitoring** task when a new alarm occurs. If **Alarm** monitoring is not in the active task list, it is added.
 - **Map (and bring to front):** Automatically switches to display alarms in the **Maps** task. If the **Maps** task is not in the active task list, it is added.
 - **Revert to original task after alarm is handled:** Automatically returns to the task you were working on before the alarm occurred after you have acknowledged the alarm.
 - **Automatically display alarm in unpacked mode:** When the alarm is triggered, displays all the attached entities of the alarm in separate tiles instead of cycling through them.
 - **Snooze time:** Sets the duration of the snooze when an alarm is put to sleep with the command.
3. Click the **Visual** tab.
4. To show the full path of the entity that triggered the alarm in the **Source** column in the **Monitoring** task and **Alarm monitoring** task, select the **Display entity names** with their full path option.
 - An entity's path is the hierarchy of areas above that entity in the area view. When the path is too long, an "*" is displayed instead.
 - **Example:** "(Honolulu office/Main entrance", or "(*/*/Back entrance".
 - **NOTE:** This option also applies to other entities. When this option is selected, the full path of other entities is shown in tile toolbars.
5. Click **Save**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 347 of 430

3.12.27 Alarm Report

Use the **Alarm Report** task to search for and investigate current and past alarms. [Figure 196](#) shows the **Alarm Report** task.

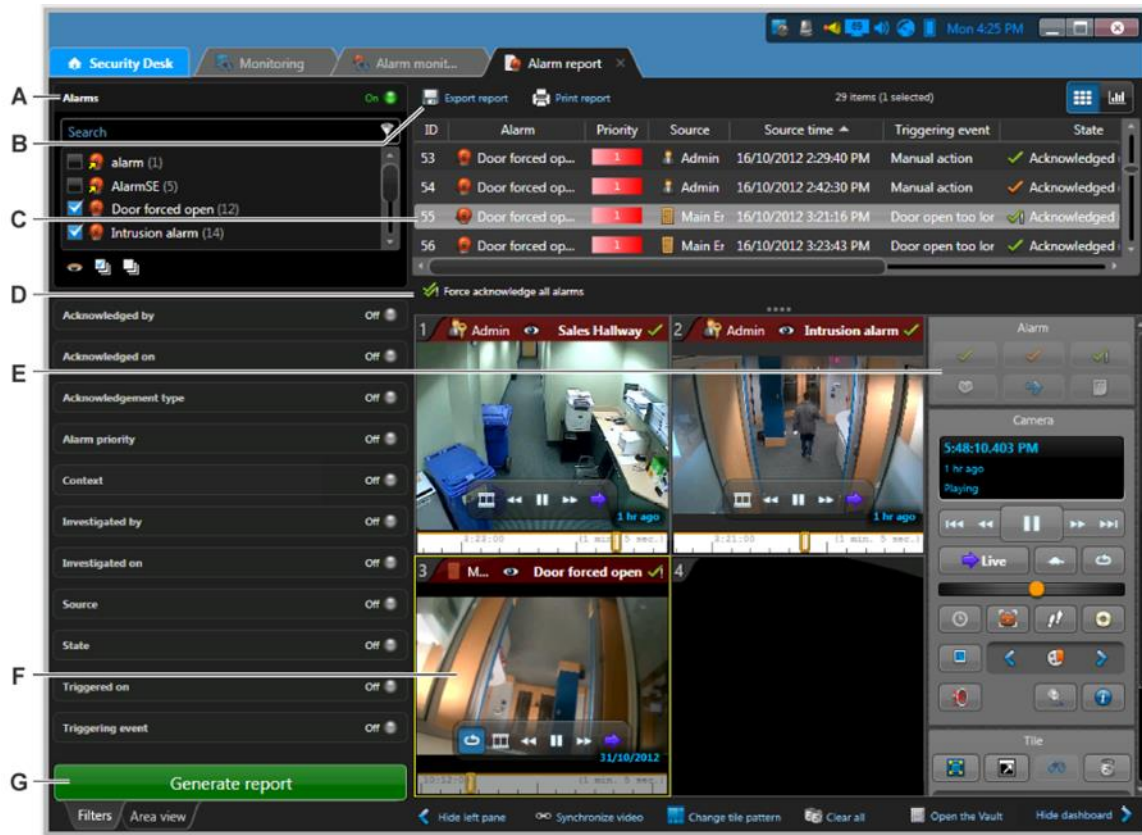


Figure 196. Genetec Security Desk – Alarm Report Task

The letters below correspond to those in [Figure 196](#).

- A. Query filters
- B. Export or print the report
- C. The alarm report results are listed in the report pane. **Right-click** an alarm to go to the **Configuration** page of the alarm or its source entity.
- D. Forcibly acknowledge all active alarms
- E. Alarm widget
- F. Video of an alarm in a tile
- G. Run the report

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 348 of 430

Query filters: Search all alarms triggered over the last day.

Query Results: Can be printed, exported or played back for review.

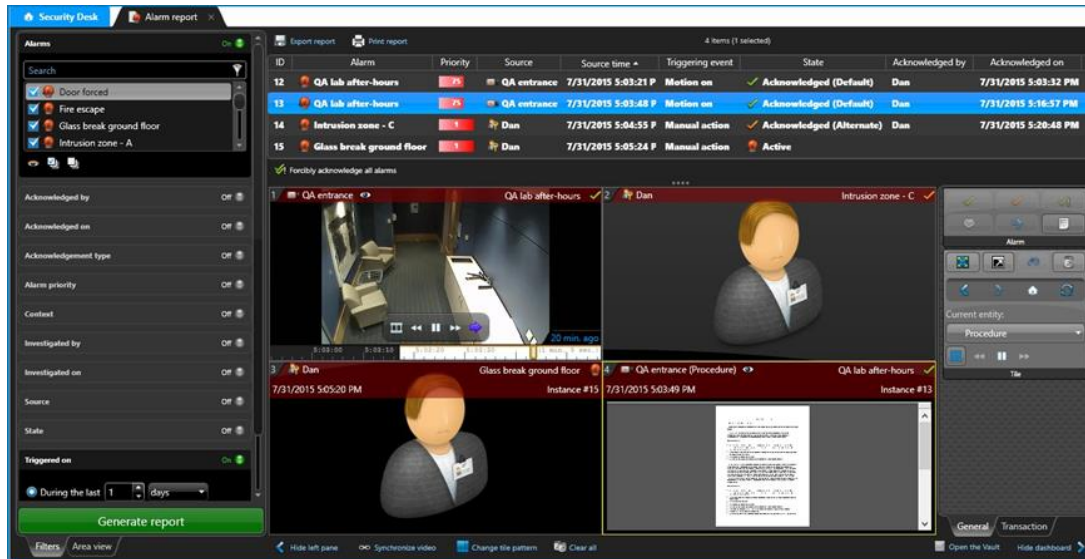


Figure 197. Alarm Management: Alarm Report

3.12.28 Report Pane Columns for the Alarm Report Task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **NOTE:** If you generated the **Alarm** report using Web Client, not all of the report columns are available.
- **ID:** Alarm instance number. Uniquely identifies each alarm instance.
- **Alarm:** Alarm entity name.
- **Priority:** Alarm priority. All alarms imported from Omnicast have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.
- **Alarm color:** Color of the alarm.
- **Source:** The source entity that triggered the alarm, when the alarm is triggered by an event-to-action. It shows a username when the alarm is triggered manually.
- **Source time:** Time of the alarm-triggering event. The only time Source time and Triggering time are different is when the event occurred while the access control unit was offline.
- **Triggering event:** Event that triggered the alarm (if triggered through an event-to-action). Manual action is indicated when the alarm was manually triggered by a user.
- **State:** Current state of the alarm.
 - **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the report pane.
 - **Acknowledged (Default):** Alarm was acknowledged using the default mode.
 - **Acknowledged (Alternate):** Alarm was acknowledged using the alternate mode.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 349 of 430

- **Acknowledged (Forcibly):** Alarm was forced to be acknowledged by an administrator.
- **Under investigation:** Alarm that is under investigation, meaning that someone has seen it but not necessarily able to take care of it.
- **Acknowledgement required:** Alarm with an acknowledgement condition that was cleared and that is ready to be acknowledged.
- **Acknowledged by:** User who acknowledged the alarm. When the alarm is acknowledge automatically by the system, Service is indicated.
- **Acknowledged on:** Time the alarm was acknowledged.
- **Context:** Alarm annotation.
- **External instance ID:** Only for federated alarms. The original alarm instance ID on the federated system.
- **Investigated by:** The user who put the alarm into the under investigation state.
- **Investigated on:** The timestamp when the alarm was put into the investigation state.
- **Occurrence period:** Period when the event occurred.
- **Trigger time:** Time the alarm was triggered in Security Center.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.

3.12.29 Operational Alarms

Operational alarms are those that have an operational impact on the specific COM-domains. Document HNL-60314 provides a catalog of “operational alarms” received and handled by the ICCS. The operation events/alarms related to COM-domains (PIS, CCTV, TS, ACS/IDS, OBS) are received by the ICCS by direct integration with each COM-domains and C-ATC.

Operational alarms are configured to automatically trigger CCTV live streams with specific pan-tilt-zoom (PTZ) preset coordinates on the video wall and/or trigger a PIS predefined message on a specified area. Once a device alarm/event is received by the ICCS GSC, the operational status of the device is updated on the graphical map on which it is displayed. At the moment of the alarm, a visual and an audible signal is activated on the operator workstations. [Figure 198](#) shows the event/alarm flows from devices to the ICCS. The flow of alarms is identified by paths with the same number.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 350 of 430

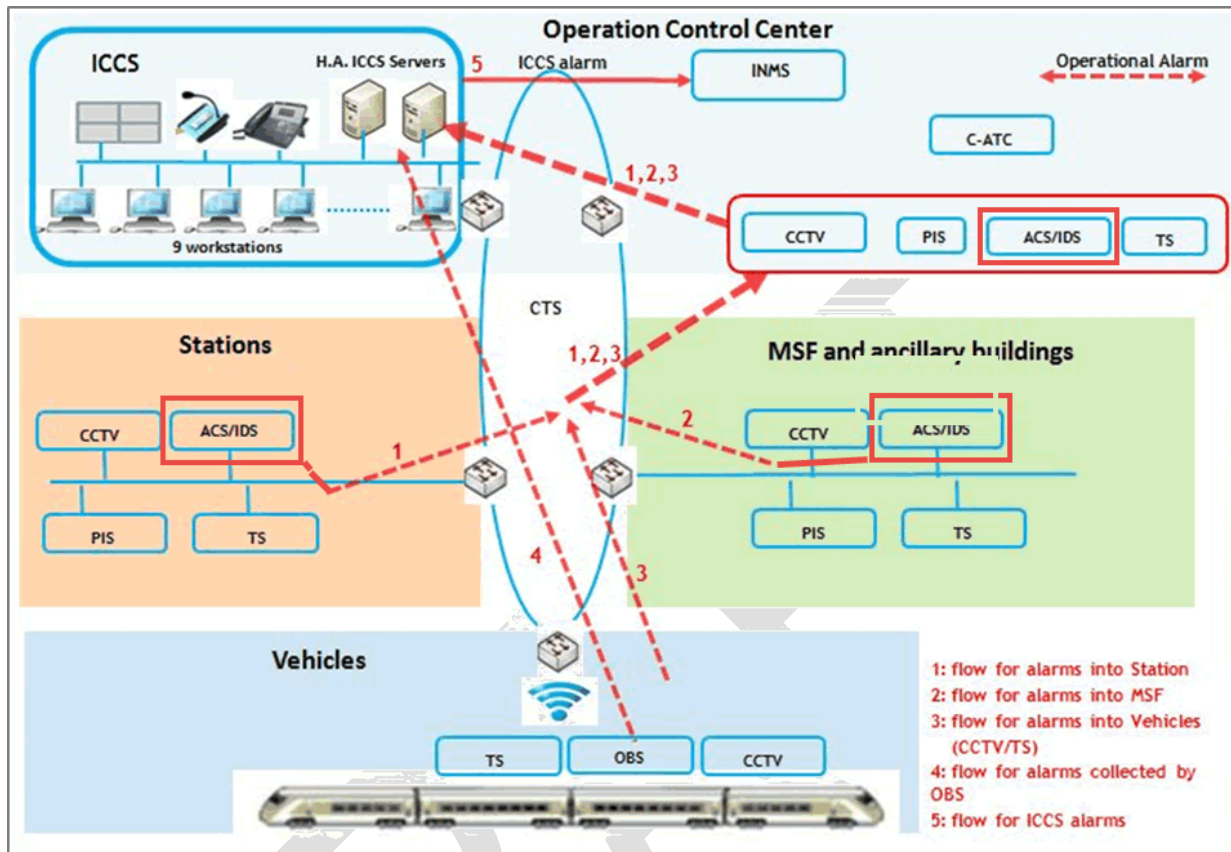


Figure 198. Event/Alarm Flows

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 351 of 430

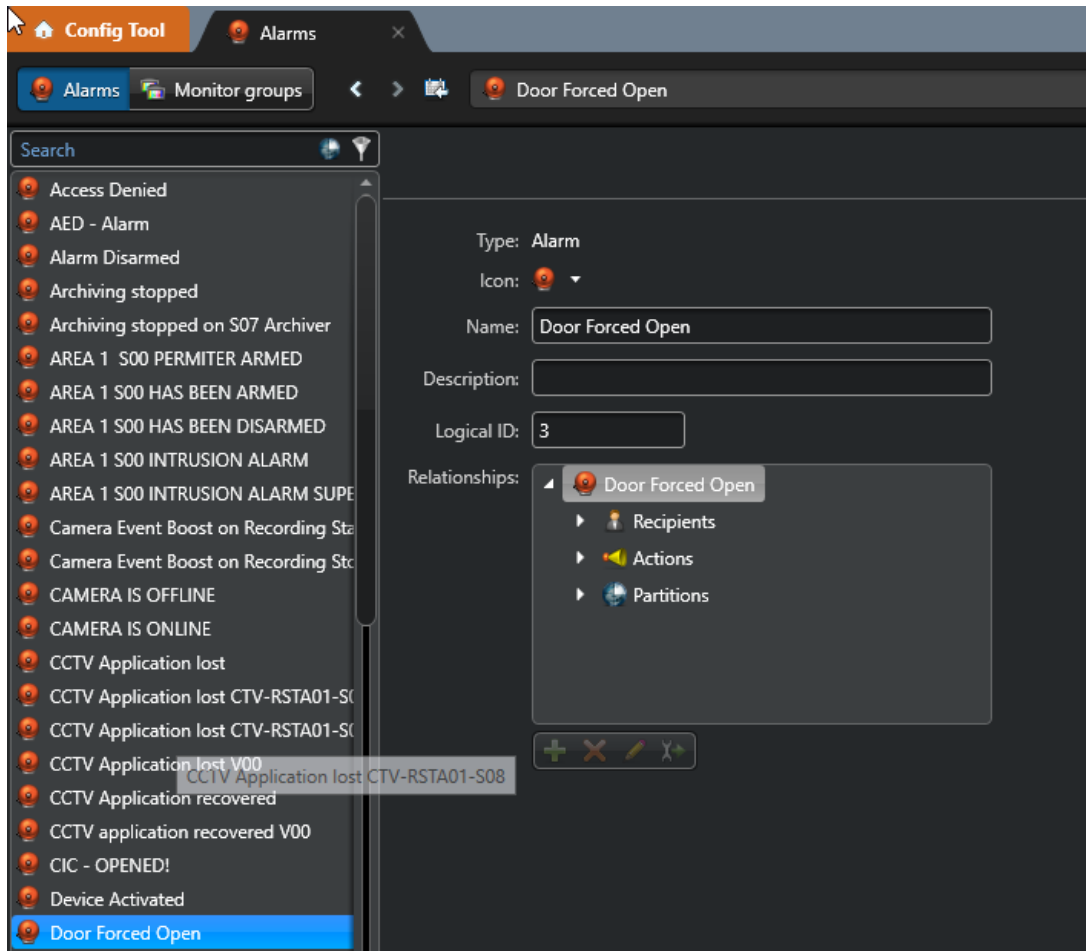


Figure 199. Alarm Management: Operational Alarms

3.12.30 Genetec Alarms, Incident and Threat Levels

A list of alarms that Genetec receives from CCTV, ACS and IDS is available in [Appendix A](#).

Threat levels indicate a potentially dangerous situation, such as a fire or gunman in the area. Threat levels are not currently assigned. Priority levels (individual user levels and authorities) are set for CCTV; however, they are not currently set for ACS or IDS.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 352 of 430	

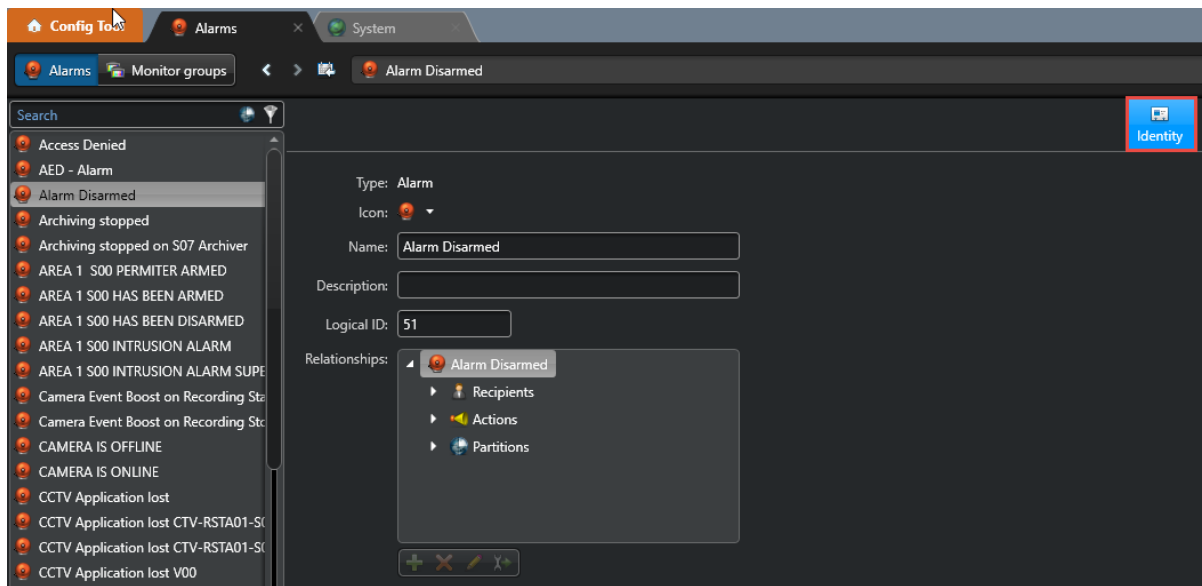


Figure 200. Alarm Management: Genetec Alarms

3.12.30.1 Corrective Actions

Operators must acknowledge every alarm. For threat alarms, operator must create an alarm report and forward it via email to the immediate manager/supervisor for decision and/or further actions.

3.12.31 Investigating Current and Past Alarms

You can search for and investigate current and past alarms, using the Alarm report task. For example, you might want to see which alarms were triggered during the last week, or since your last shift. You could search for major events that happened in your system, by only selecting critical alarms. You can see who acknowledged a specific alarm, and why. If there was a critical alarm that occurred and you must re-examine it, you can search for the alarm, and then review the attached video. If needed, you can also export the alarm video, and send it to law enforcement as evidence.

To investigate an alarm:

- From the home page, open the **Alarm report** task.
- Set up the query filters for your report. Choose one or more of the following filters:
 - Alarms:** Select the types of alarms you want to investigate. Alarms can be locally defined, or imported from federated systems.
 - Acknowledged by:** Users who acknowledged the alarm.
 - Acknowledged on:** Alarm acknowledgement time range.
 - Acknowledgement type:**
- Select one of the following acknowledgement type options:
 - Alternate:** Alarm was acknowledged by a user using the alternate mode.
 - Default:** Alarm was acknowledged by a user, or auto-acknowledged by the system.
 - Forcibly:** An administrator forced the alarm to be acknowledged.
 - Alarm priority:** Alarm priority.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 353 of 430

NOTE: All alarms imported from Omnicast have their priority set to 1 by default. You can change their priority at a later time in the Config Tool.

- **Context:** Restrict the search to alarms with a specific text in the annotation. The search is case insensitive.
 - **Investigated by:** Which user put the alarm into the under investigation state.
 - **Investigated on:** Specify a time range when the alarm was put into the under investigation state.
 - **Source:** Source entity that triggered the alarm in the case of an event-to-action, or the user who triggered the alarm manually.
 - **State:** Current state of the alarm.
 - **Active:** Alarm is not yet acknowledged. Selecting an active alarm shows the alarm acknowledge buttons in the report pane.
 - **Acknowledged:** Alarm was acknowledged by a user, or auto-acknowledged by the system.
 - **Under investigation:** Alarm that is under investigation.
 - **Acknowledgement required:** Alarm with an acknowledgement condition that was cleared is ready to be acknowledged.
 - **Triggered on:** Alarm trigger time range.
 - **Triggering event:** Events used to trigger the alarm.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
6. Click **Generate report**. The alarms are listed in the report pane.
 7. To show the corresponding video of an alarm in a tile, double-click or drag the item from the report pane to the canvas.
 8. To control the alarms, use the alarm widget. The alarms are listed in the **report** pane.
 9. To show the corresponding video of an alarm in a tile, double-click or drag the item from the report pane to the canvas.
 10. To control the alarms, use the alarm widget.

3.13 REPORTS

This section describes different reports available in Security Center.

3.13.1 Reporting Task Workspace

Reporting tasks are where you generate customized queries about the entities, activities, and events in your *Security Center* system for investigation or maintenance purposes. Most investigation and maintenance tasks are reporting tasks.

This section takes you on a tour of the reporting task layout and describes the common elements of most reporting tasks. The **Area activities** task was used as an example. You can open the **Area activities** task by typing its name in the **Search** box on the home page.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 354 of 430

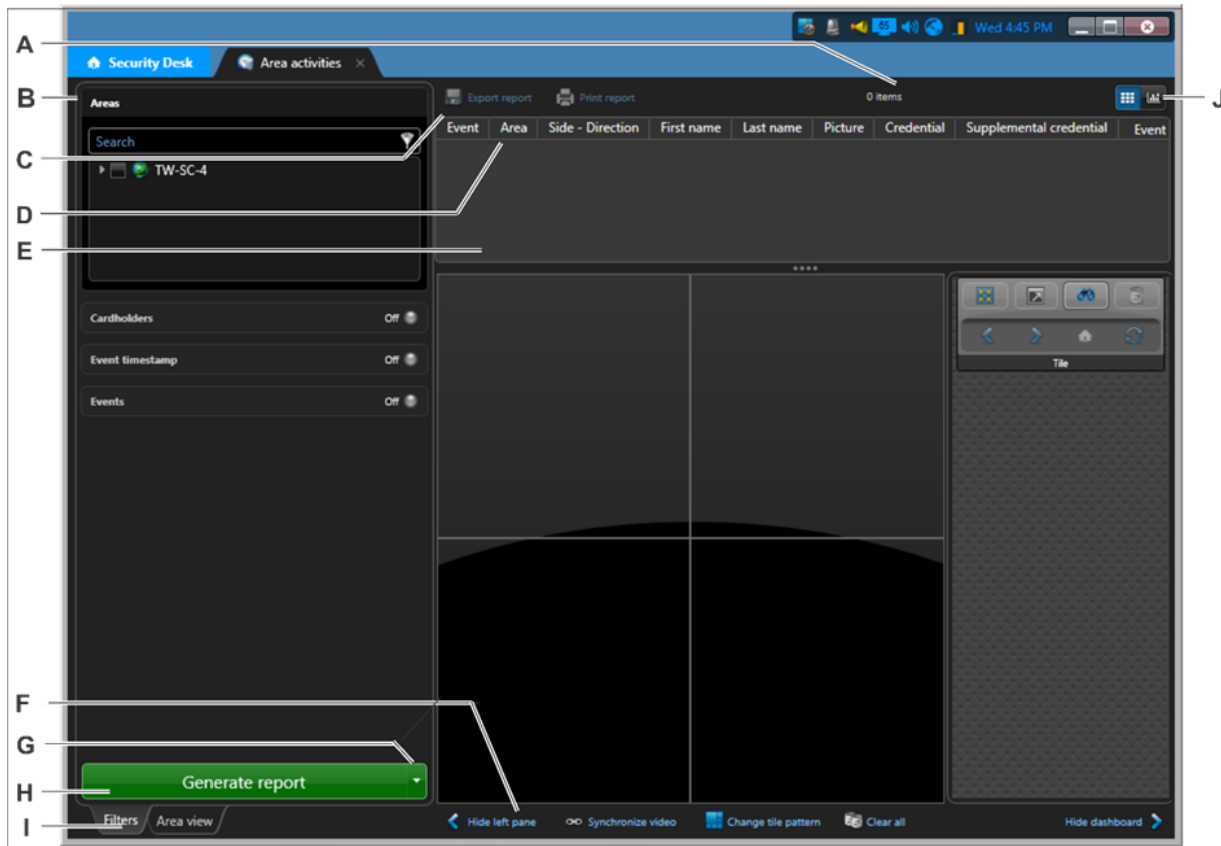


Figure 201. Security Desk – Area Activities Task

The letters below correspond to those in [Figure 201](#).

- A. **Number of results:** Displays the number of returned results. A warning is issued when your query returns too many rows. If this happens, adjust your query filters to reduce the number of results.
- B. **Query filters:** Use the filters in the **Filters** tab to set up your query. Click on a filter heading to turn it on () or off. Invalid filters display as **Warning** or **Error**. Hover your mouse over the filter to view the reason it is invalid.
- C. **Export or print report:** Click to export or print your report once it is generated.
- D. **Select columns:** Right-click a column heading to select which columns to display in the report pane.
- E. **Report pane:** View the results of your report. Drag an item from the list to a tile in the canvas, or right-click an item in the list to view more options associated with that item, if applicable (such as launching another report related that report result).
- F. **Tile commands:** Commands related to canvas tiles:
 - **Synchronize video:** Synchronize the video that is displayed in the canvas.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 355 of 430

- **Clear all:** Empty all content from tiles.
 - **Change tile pattern:** Change the tile pattern in the canvas.
- G. **Generate and save report:** Click to run and save the report directly to a file (**PDF**, **CSV**, or **Excel** format). This button is disabled if you have not selected any query filters, or when you have invalid filters.
- H. **Generate report:** Click to run the report. This button is disabled if you have not selected any query filters, or when you have invalid filters. While the query is running, the button changes to **Cancel**. Click on **Cancel** to interrupt the query.
- I. **Filters tab:** Use the **Filters** tab to customize and filter your searches. The **Filters** tab only appears in reporting tasks.
- NOTE:** Click the **Area view** tab to show the area view and select entities to view in the canvas.
- J. **Tiles or Charts:** If the report supports tiles, open the chart view using the **toggle** button  at the top right of the task. Otherwise, open the chart view using the **Charts** button .
- If the report supports tiles: Click the **Tiles** button  to show the **Tiles** view below the report pane.
 - If the report supports charts: Click the **Charts** button  to show the **Charts** view below the report pane.

3.13.2 About Visual Reports

Visual reporting is dynamic charts or graphs in *Security Desk* that deliver insights visually that you act on. You can perform searches and investigate situations using these visual and user-friendly reports. The visual report data can be analyzed to help identify activity patterns and enhance your understanding.

Visual reports can display data in a graph or chart format along a specified axis by using lines or bars to visually represent the report data. The X axis represents all the labels (group by), and the Y axis shows the total number of instances relative to the X axis.

On the X axis, two types of grouping can be achieved:

- **Nominal values:** Can separate the data in multiple columns on the X axis. For example, the X axis values can be sorted by the number of instances, and the user can choose the grouping (Top 3, Top 5, or Top 10).
- **Dates:** Can separate the X axis based on a timeline. For example, the user can change the date interval grouping (Hour, Day, Week, Month, or Year).

Visual chart types

The following chart types are supported in *Security Center v5.7* when using the **Generate report** functions in *Security Desk*: **Lines**, **Columns**, **Stacked columns**, **Rows**, **Stacked rows**, **Doughnut**, and **Pie**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 356 of 430

3.13.2.1 Lines Chart

Use a **Lines** chart (📈) when you want to track changes over a short or long period of time. For example, the total instances of the selected report data in relation to a timeline.

- Line charts can represent the data better than row or column charts when the difference in changes is small.
- Line charts can also be used to compare changes over the same period for more than one group.

The following example shows a **Cardholder events** report, Split by: **First name**, Show: **Top 5** and X-Axis: **Event timestamp**, Group by: **Day** as a **Lines** chart.

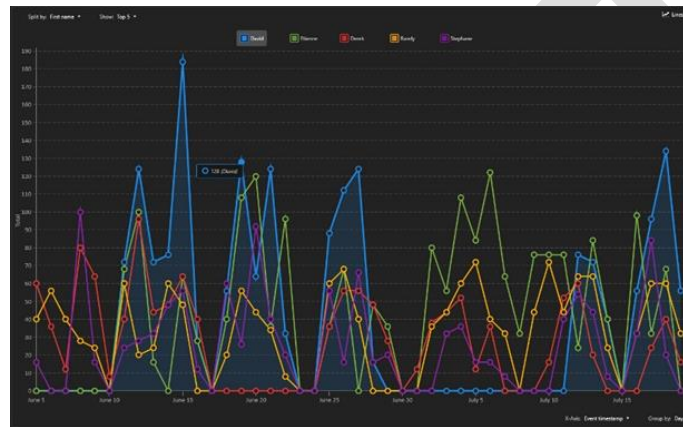


Figure 202. Reports: Line Charts: Cardholder Event Report

3.13.2.2 Lines Chart (Simplified)

When the time range is too wide or too precise, a lot of data has to be computed and displayed on screen. In this situation, a simplified version of the lines chart is displayed. The following example shows a simplified version of a **Lines** chart (📈).

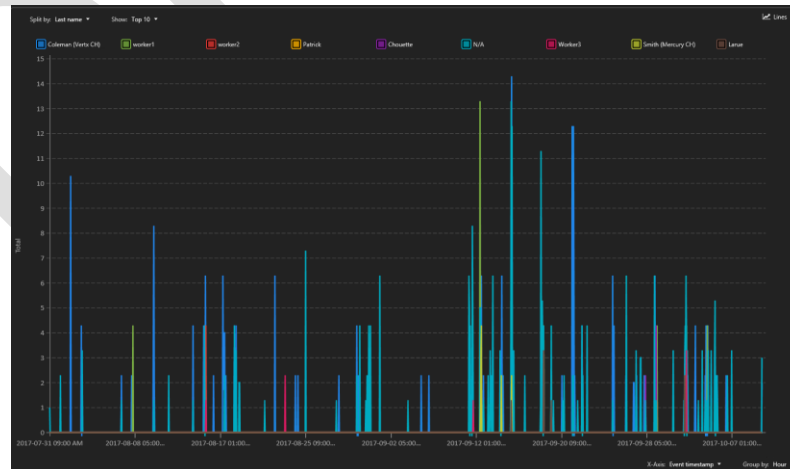


Figure 203. Reports: Simplified Line Chart

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 357 of 430

NOTE: The simplified version of a lines chart does not support interaction with the mouse or indication of Y value for a specific point.

3.13.2.3 Columns Chart

Use a **Columns** chart (📊) when you want to group the data by category and display the results using vertical bars.

The following example shows a **Door access** report, Split by: **Event**, Show: **Top 10** and X-Axis: **Door**, show: **Top 10** as a **Columns** chart.

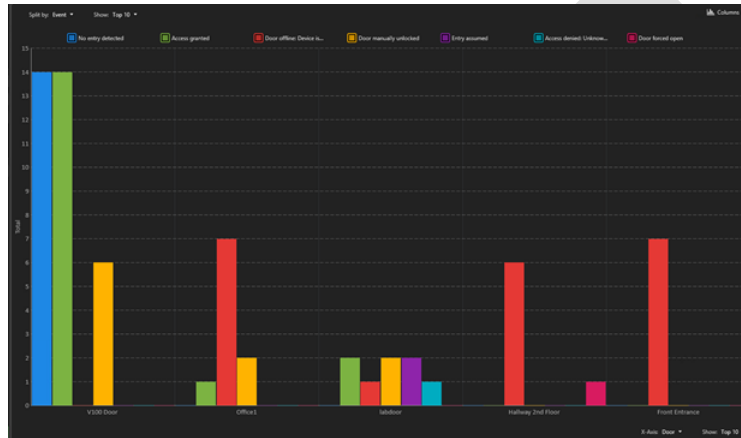


Figure 204. Reports: Column Chart: Door Access Report

3.13.2.4 Stacked Columns Chart

Use a **Stacked** columns chart (📊) when you want to group the data by category and display the results using vertical bars. The Y axis can be used to split the data and have more precise information in relation to the X value.

The following example shows a **Door activities** report, Split by: **Event**, Show: **Top 10** and X-Axis: **Door**, Show: **Top 10** as a **Stacked columns** chart.

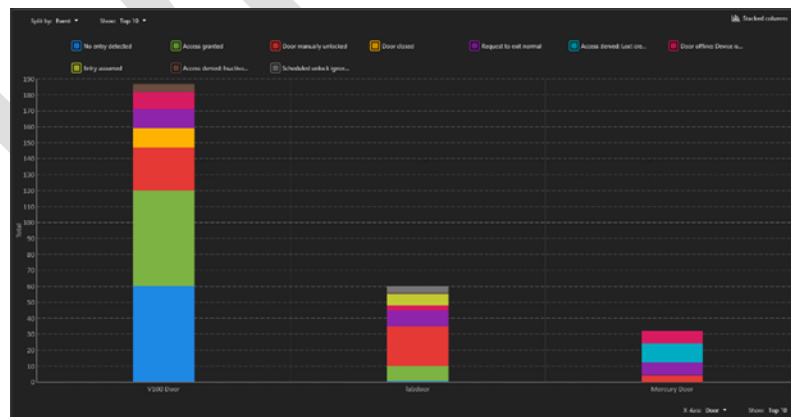


Figure 205. Reports: Stacked Columns: Door Activities Report

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 358 of 430	

3.13.2.5 Rows Chart

Use a **Rows** chart (📊) when you want to group the data by category and display the results using horizontal bars. The following example shows an Intrusion detector report, Y-Axis: **Camera**, Show: **Top 10** and Split by: **Frame time**, Group by: **Hour**, Show: **Top 10** as a **Rows** chart.

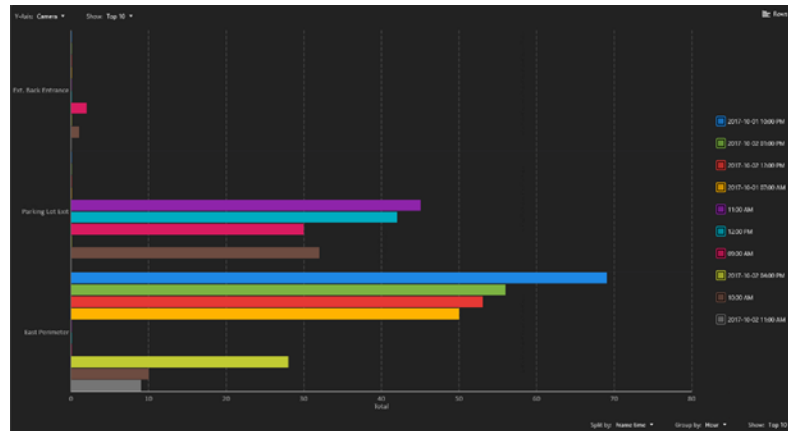


Figure 206. Reports Rows: Intrusion detector report

3.13.2.6 Stacked Rows Chart

Use a **Stacked rows** chart (📊) when you want to group the data by category and display the results using horizontal bars. The X axis can be used to split the data and have more precise information in relation to the Y value.

The following example shows an Intrusion detector report, Y-Axis: **Camera**, Show: **Top 10** and Split by: **Frame time**, Group by: **Hour**, Show: **Top 10** as a **Stacked rows** chart.

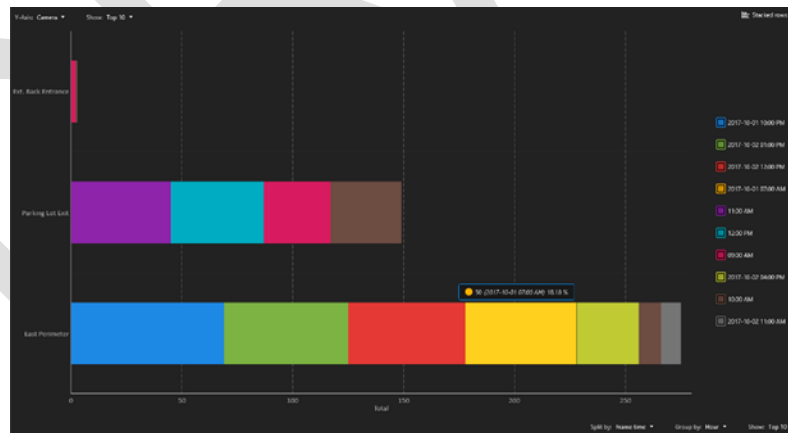


Figure 207. Reports: Stacked Rows: Intrusion Detector Report

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 359 of 430

3.13.2.7 Pie and Doughnut Charts

Use a **Pie or Doughnut** chart when you want to compare report data as a whole.

NOTE: Pie or Doughnut charts do not show changes over time.

Pie chart (📊) The following example shows a **Camera events motion** report, Data: **Camera**, Show: **Top 10** as a **Pie** chart.

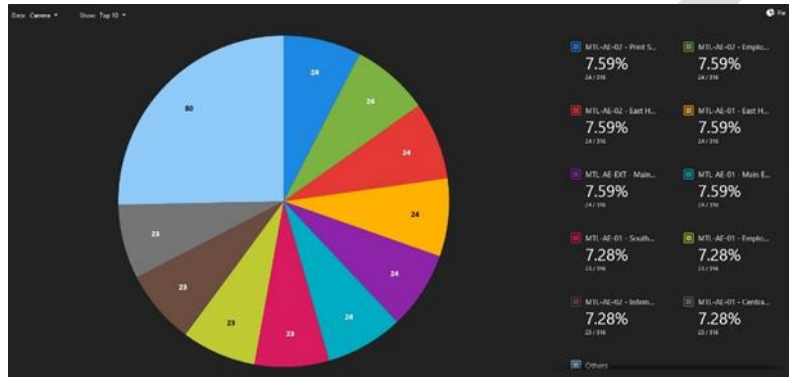


Figure 208. Pie Chart: Camera Events and Motion Report

3.13.2.8 Doughnut Chart

The following example shows a **Camera events** report, Data: **Camera**, Show: **Top 10** as a **Doughnut** chart (📊).



Figure 209. Doughnut Chart: Camera Events and Motion Report

3.13.3 Generate a Report

To generate a report in any reporting task, you must set the query filters, and then run the query. After you generate the report, you can work with your results.

Reporting tasks are where you generate customized queries about the entities, activities, and events in your *Security Center* system for investigation or maintenance purposes. Most investigation and maintenance tasks are reporting tasks.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 360 of 430

The maximum number of report results you can receive in *Security Center* is 10,000. By default, the maximum number of results is 2000. This value can be changed from the **Options** dialog box. If you want to generate a report with more than 10,000 results, then use the **Generate** and **save** report command.

- **NOTE:** These steps only describe the general process for running a report.

To Generate a Report:

1. Open an existing reporting task or create a new one.
2. In the **Filters** tab, use the query filters to create a customized search.

NOTE: Some of the filters have a **Select all** button. This button does not appear if there are more than 100 entities to select from (for example, if you have a list of 1500 cardholders), because if you query too many entities the report takes too long to generate.

3. Set a date and time range for the report.
4. Click **Generate report**.

If there are invalid filters, the **Generate report** button is unavailable.

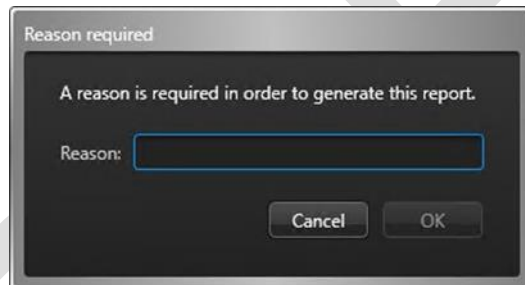


Figure 210. Reports: Reason Required Dialog

This ensures that the reason for the LPR search is logged and included in **Activity trail** (Report generated) audit logs to comply with State laws.

The query results are displayed in the report pane.

TIP: You can sort the results by column. You can also right-click the titles row to select columns, then add or remove columns as required.

5. Analyze the query results.

The query results depend on the type of reporting task. When video sequences or LPR data are attached to the query results, you can view them in the canvas by dragging a report item to a tile.

6. Work with the query results. Depending on the items in the query results, you can print the report, save the report as an Excel or PDF document, export the video sequences, and so on.
7. Optional: Save the report as a template.

If you save the report layout (query filters and report columns) as a template, it can be sent to another user or workstation using the **Email a report** action.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 361 of 430

3.13.3.1 Select Date and Time Ranges For Reports

You can specify a date time range to filter your report queries.

If the time range is invalid, an error icon (❌) appears, and you cannot generate the report. When the time range covers multiple days, a warning icon (⚠️) appears on the filter, informing you the report might take longer to generate.

- **IMPORTANT:** If you have a larger system that includes devices operating in different time zones, your time range filters are affected.

To Select and Date and Tme Range for a Report:

1. Open an existing reporting task or create a new one.
2. In the **Time range** section, select one of the following time range modes:

NOTE: Depending on the reporting task you are using, this filter might be called **Triggered on** or **Event timestamp**.

- **During the last:** A relative time range using the last number of seconds, minutes, hours, days, weeks, months, or years. The report results will be different every time, since the time range is based on the current time.
 - **Specific range:** An absolute date and time range using From and To fields. The same report results will be produced every time you run the query.
3. If you select the **Specific range time range** mode, edit the **From** and **To** fields as follows:
 - A. Next to the **From** or **To** fields, click **Start** or **Now**.
 - B. To change the date, click the arrow, and then select a date in the calendar.
You can zoom out to view multiple years by clicking the calendar heading or zoom in by clicking the year or month.
 - C. To specify a time, click the **Set time** link, and then enter the time directly in the **time** fields.

3.13.4 Export a Generated Report

In every reporting task, you can export your report after it is generated. To export the report data as a list (**CSV**, **Excel**, or **PDF** format) use the **Data** option. To export the report data as a chart (**JPEG** or **PNG**) use the **Graph** option. Alternatively, you can select both options to generate a report list and chart. The maximum number of report results that can be exported is 10,000.

To Export a Generated Report:

1. At the top of the report pane, click **Export report** (📄).
2. In the dialog box, select either **Data**, **Graph**, or both and set the following options:
 - **File format:** (Data only) Select the file format (**CSV**, **Excel**, or **PDF**). (Graph only) Select the file format (**JPEG** or **PNG**).
 - **Destination file:** Select the file name.
 - **Orientation:** (PDF only) Select whether the PDF file should be in portrait or landscape mode.
 - **Attached files folder:** (CSV only) Specify where the attached files, such as cardholder pictures or images, are saved.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 362 of 430

NOTE: The dialog box options that are displayed can vary depending on whether the report supports Charts (Graph) or not. The **Charts** function is not supported for the following reports: **Door Troubleshooter**, **Video File Explorer**, and **Motion Search**.

3. Click **Export**.

3.13.4.1 Print A Generated Report

In every reporting task, you can print your report after it is generated. To print the report data as a list, use the **Print data** option. To print a visual report or chart use the **Print graph** option.

NOTE: NitroPdf is not currently supported.

To print a report (Print data):

1. At the top of the report pane, click **Print report** (🖨️) then click **Print data**.
2. In the **Report preview** window, click **Print**, and select a printer.

TIP: You can also export (📄) the **Report preview** as a Microsoft Excel, Word, or Adobe PDF document.

To print a visual report (Print graph):

3. At the top of the report pane, click **Print report** (🖨️) then click **Print graph**.
4. In the **Print window**, select a printer and click **Print**.

3.13.5 Generating Visual Reports

To generate a visual report in any reporting task, you must set the query filters, and then run the query. After you generate the report, you can work with your results using charts and graphs.

- You must have a visual reports license to use the charts function in reports.
- Only users with the view charts privilege can access the visual report charts.

Reporting tasks are where you generate customized queries about the entities, activities, and events in your *Security Center* system for investigation or maintenance purposes. Most investigation and maintenance tasks are reporting tasks. Here are some visual reporting use case examples:

- **Omnicast™ Camera events task:** View camera reports as charts to understand activity on multiple cameras, during a specified period.
- **Synergis™ Door activities:** View events as charts and graphs to gain insights about your access control system.
- **NOTE:** The Charts function is not supported for the following reports: **Door Troubleshooter**, **Video File Explorer**, and **Motion Search**.

To Generate a Visual Report:

1. Open an existing reporting task that supports the charts function or create a new one.
2. In the **Filters** tab, use the query filters to create a customized search.
 - **NOTE:** Some of the filters have a Select all button. This button does not appear if there are more than 100 entities to select from (for example, if you have a list of 1500 cardholders), because if you query too many entities the report takes too long to generate.
3. Set a date and time range for the report.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 363 of 430

4. Click **Generate report**. If there are invalid filters, the **Generate report** button is unavailable.
5. The query results are displayed in the **report** pane.
 - **TIP:** You can sort the results by column. You can also right-click the titles row to select columns, then add or remove columns as required.
6. Do one of the following:
 - If the report supports tiles, open the chart view using the **toggle** button () at the top right of the task.
 - If the report does not support tiles, open the chart view using the **Chart** button ().
7. Select a **Chart** type from the drop-down menu in the **Charts** pane.

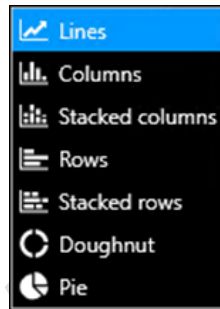


Figure 211. Reports: Chart Type Dropdown Menu

8. Select the data that you want displayed in the visual report using the drop-down menus in the Charts pane: Split by, Show (**Top 10**, **Top 5**, or **Top 3**), X-Axis, Y-Axis, or Data.
 - **NOTE:** Only the drop-down menus that are relevant to the chart selected are displayed. The choices available in the drop-down menus vary depending on the data in the report pane.
 - **Example:** The following example shows the **Top 10** camera events as a **Doughnut** chart.

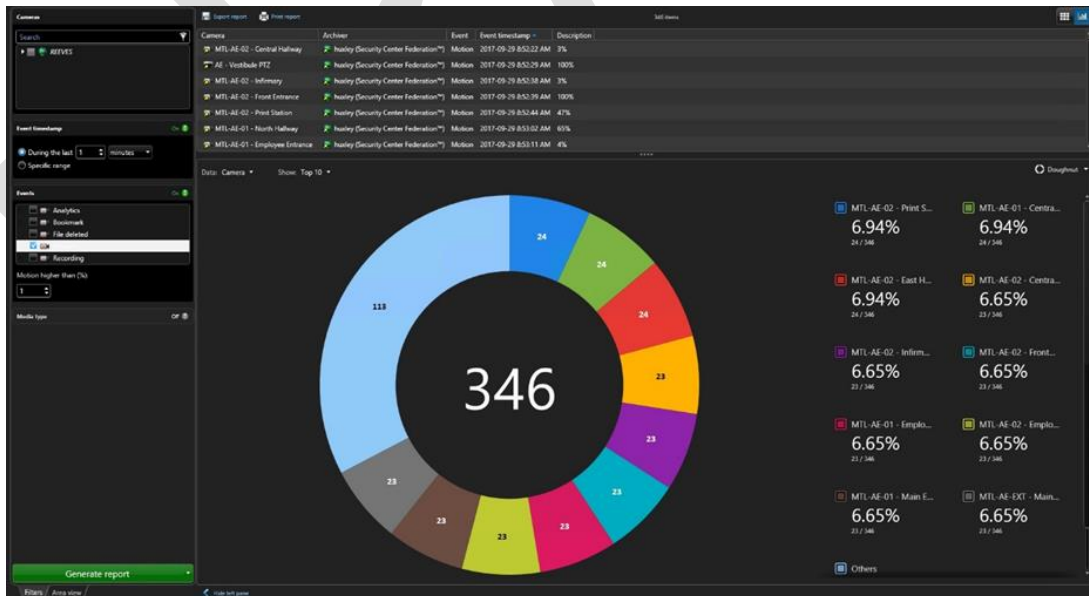


Figure 212. Reports: Donut Chart: Top 10 Camera Events

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 364 of 430

- **Example:** The following example shows the **Top 5** cardholder events split by **First Name** and **Event timestamp** grouped by **Day** over a specified period as a **Lines** chart.

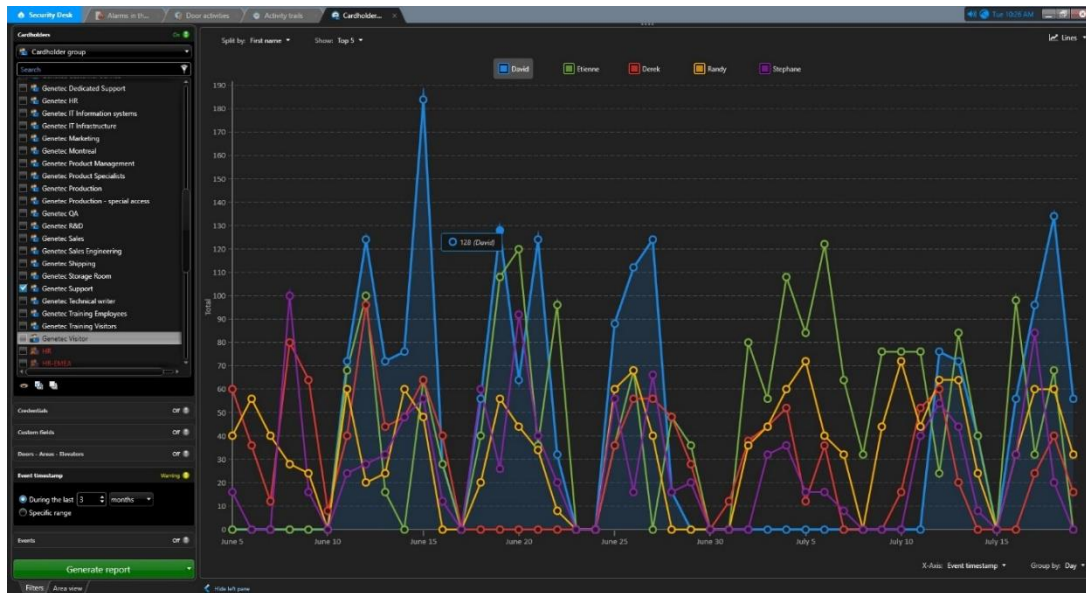


Figure 213. Reports: Line Chart: Top 5 Cardholder Events

9. (Optional) Manipulate the data in the chart.
 - You can hover over elements in the graph or chart to display additional information, this also highlights the related item in the chart legend.
 - **TIP:** You can quickly show or hide data in the chart by selecting  or clearing  a chart legend item.
10. Analyze the query results. The query results vary depending on the type of reporting task.
11. Work with the query results. Depending on the items in the query results, you can export the report as data (**Excel**, **CSV**, or **PDF**) or as a Graph (**PNG** or **JPEG**). You can also print the report as data or a graph.
12. Optional: Save the report as a template.

If you save the report layout (query filters and report columns) as a template, it can be sent to another user or workstation using the **Email a report** action.

3.13.6 Generate and Save a Report

Instead of waiting for a report to generate and then exporting the results, you can generate a report and save it to a file location directly. Generating and saving a report is helpful, because you do not have to wait at your workstation for the report to generate. It is also helpful if your query has many results, because you are not limited to 10, 000 results like when you generate a report normally.

- **NOTE:** The tasks that support this command are those where the results are queried from a role database, and not the directory.

To Generate and Save a Report:

1. Open an existing reporting task or create a new one.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 365 of 430

- In the **Filters** tab, use the query filters to create a customized search.

NOTE: Some of the filters have a **Select all** button. This button does not appear if there are more than 100 entities to select from (for example, if you have a list of 1500 cardholders), because if you query too many entities the report takes too long to generate.

- Right-click** a column heading in the report pane and click **Select columns** .
- Select which columns to include in the saved report and click **Save**.
- Click the drop-down arrow next to **Generate report** and click **Generate** and **save** report.
- In the dialog box, set the following options:
 - File format:** Select the file format. Only CSV is supported.
 - Destination file:** Select the file name.
 - Orientation:** (PDF only) Select whether the PDF file should be in portrait or landscape mode.
 - Attached files folder:** Specify where the attached files, such as cardholder pictures or images, are saved.
- Click **Export**. The report is saved in the location you specified.

3.13.6.1 Generate and Save a Reports Using a System Action

You can generate and save a report using a manual action.

- Save the task that you want to generate and export as a public task, with the query filters that you want applied, and the report columns you want to include.
- Set the maximum number of report results that can be saved in PDF or Excel format, and the destination folder from the Report Manager Properties tab. For more information, see the Security Center Administrator Guide.

To Generate and Save a Report Using a System Action:

- In the notification tray, click **Hot actions** .
- In the **Hot actions** dialog box, click **Manual action**.
- In the list of actions, click **Export report**.
- From the **Report** drop-down list, select the saved public task that you want to export.
- From the **File format** drop-down list, select **PDF**, **Excel**, or **CSV**.
- (PDF only) From the **Orientation** drop-down list, select whether the PDF file should be in portrait or landscape mode.
- If you want to overwrite a report that was previously exported to the destination folder, then select the **Overwrite existing file** option.
- Click **OK**. The report is saved in the location you specified.

3.13.7 Customize the Report Pane

Once you have generated your report, you can customize how the results are displayed in the report pane.

To Customize the Report Pane:

- Generate your report.
- Choose which columns to show, as follows:

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 366 of 430

- A. In the report pane, right-click on a **column** heading, and then click **Select columns** (📄).
 - B. Select the columns you want to show and clear the columns you want to hide.
 - C. To change the column order of appearance, use the (↔) and (↔) arrows.
 - D. Click **OK**.
3. To adjust the width of a column, click between two column headings and drag the separator to the right or left.
 4. To change the column order, click and hold a column heading in the **report** pane, and dragging it to the desired position.
 5. To sort the report by one of the columns, click the **column** heading. Click the **column** heading a second time to sort the report in the reverse order.
 - **NOTE:** All columns containing timestamps are sorted according to their UTC time value. If you choose to display the times in *Security Center* according to each device's local time zone rather than a fixed time zone, the times might appear out of order if the report contains devices from different time zones.
 6. To increase the size the report pane, drag the separator bar between the **report** pane and the canvas to the bottom of the application window.
 7. Save your task layout with the changes you made to the **report** pane as follows:
 - To save the task as a **private** or **public** task, right-click the **task** tab, and then click **Save as**.
 - To save the workspace for the next time you open the application, right-click in the **taskbar**, and then click **Save workspace**.

3.13.8 Customize Report Behavior

You can select how many report results to receive, and when you want to receive error messages about reports, from the Options dialog box.

When the query reaches the specified limit, it automatically stops with a warning message. The maximum value you can set is 10,000. The report settings are saved as part of your user profile and apply to Security Desk and **Config Tool**.

To Customize Report Behavior:

1. From the home page, click **Options > Performance**.
2. In the **Reports** section, set the **Maximum number of results** option value.
This option determines the maximum number of results that can be returned by a query using a reporting task. This limit helps ensure stable performance when too many results are returned if your query is too broad.
3. Click the **User interaction** tab.
4. If you want *Security Center* to display a warning message every time you are about to execute a query that might take a long time, select the **Display warning** if query may take a long time to execute option.
5. Click **Save**.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 367 of 430

3.13.9 Set Maximum Report Results for Automated Reports

You can select the maximum number of results that can be generated using the **Email a report** or **Export report** actions, to prevent report that has too many results from freezing your computer. The maximum number of results only applies if you are saving the report in PDF or Excel format. It does not apply to CSV format.

The **Email a report** or **Export report** actions can be triggered using event-to-actions or triggered as a one-time action or hot action from *Security Desk*.

To Set the Maximum Number of Report Results:

1. From the **Config Tool** home page, open the **System** task, and click the **Roles** view.
2. Select the **Report Manager** role, and click the **Properties** tab.
3. Set a value in the **Maximum number of results for batch reports** option and click **Apply**.

3.14 SYSTEM TOOLS

Security Center offers 9 tools to create reports with. The nine tools are as follows:

- Access Troubleshooter Tool
- Unit Enrollment Tool
- Unit Replacement Tool
- Move Unit Tool
- Copy Config Tool
- Upgrade Firmware
- Database Actions
- Diagnostic Data Collection Tool
- Import Tool

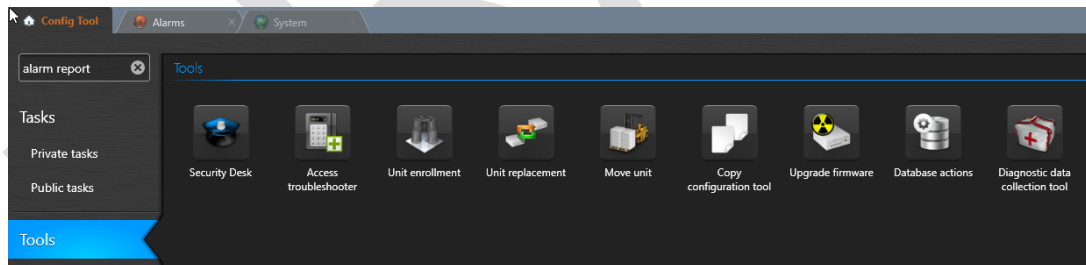


Figure 214. Security Center Tools

3.14.1 Access Troubleshooter Tool

The **Access troubleshooter** tool allows you to test and troubleshoot your access control system after it is set up, such as your access rules, and door configurations.

If you have a large system, you might have multiple schedules (Office hours/Office closed/Holidays/Weekends/Special events), multiple areas and sub-areas, multiple cardholder groups, and so on. As you build your system, and continue to create entities, the basic access logic applied at a door can become more difficult to determine.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 368 of 430

You can use the **Access troubleshooter** to find out the following:

- Who is allowed to pass through an access point at a given date and time
- Which access points a cardholder is allowed to use at a given date and time
- Why a given cardholder can or cannot use an access point at a given date and time

The Access troubleshooter is most accurate when examining an event that just occurred. When using the troubleshooter to investigate a past event (for example, an access denied event), keep in mind that your settings might have changed since that event occurred. The troubleshooter does not take past settings into consideration. It only evaluates a situation based on the current settings.

3.14.2 Unit Enrollment Tool

The Unit enrollment tool allows you to discover IP units (video and access control) connected to your network, based on their manufacturer, and network properties (discovery port, IP address range, password, and so on). Once discovered, the units can be added to your system.

The Unit enrollment tool allows you to discover IP units (video and access control) connected to your network, based on their manufacturer, and network properties (discovery port, IP address range, password, and so on). Once discovered, the units can be added to your system.

The Unit enrollment tool opens automatically after the *Security Center* installer assistant unless you cleared the Open the **unit enrollment** tool after the **wizard** option.

When adding access control units, only HID and Synergis™ units can be enrolled with Unit enrollment tool. For complete details on how to enroll Synergis™ units, see the *Synergis™ Appliance Configuration Guide*.

3.14.2.1 Configure Unit Enrollment Settings

You can use the **Settings and manufacturers** button in the **Unit enrollment** tool to specify which manufacturers to include when searching for new units. You can also configure the discovery settings for units and specify username and passwords for units so they can be enrolled easily.

To Configure Your Discovery Settings:

1. From the home page, click **Tools > Unit enrollment**.
2. In the **Unit enrollment** dialog box, click **Settings and manufacturers** (⚙️).
3. Configure the following options:
 - **Always run extensive search.** Turn this on if you want all units on the system to be discovered.
NOTE: Units from other manufacturers may also be discovered because UPnP and Zero config are also used in the discovery process.
 - **Refuse basic authentication (video units only).** Use this switch to enable or disable basic authentication. This is useful if you turned off basic authentication in the *Security Center InstallShield*, but you need to turn it back on to perform a firmware upgrade, or enroll a camera that only supports basic authentication. To turn basic authentication back on, you must switch the **Refuse basic authentication** option to **Off**.

NOTE: This option is only available to users with **Administrator** privileges.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 369 of 430

4. Click **Add manufacturer** (+) to add a manufacturer to the list of units that will be discovered. To delete a manufacturer from the list, select it and click (X).
5. Configure the individual settings for any manufacturers you added. To do this, select the manufacturer and click (Pencil icon).

IMPORTANT: You must enter the correct username and password for the unit to enroll properly.

6. (Optional) Remove units from the list of ignored units.
7. Click **Save**.

3.14.2.2 Discover Units on Your Network

If you do not know the IP address of the video or access control unit you want to add, you can find the unit on your network using the Unit enrollment tool.

To Discover Units:

1. From the **home** page, click **Tools > Unit enrollment**.
2. Configure your unit enrollment settings.
3. Click **Save > Start discovery** (Start icon).

The units discovered on your network are listed, using the enrollment settings you configured for each manufacturer. You can stop the discovery process at any time.

3.14.2.3 Add a Unit

Once new units have been discovered, you can use the **Unit enrollment** tool to add them to your system.

To add a unit:

1. From the **home** page, click **Tools > Unit enrollment**.
2. There are three ways to add newly discovered units:
 - Add all the new discovered units at the same time by clicking the **Add all** () button at the lower right side of the dialog box.
 - Click on a single unit in the list, then click **Add** in the **Status** column
 - **Right-click** a single unit from the list and click **Add** or **Add Unit**.

When a video unit does not have the correct *username* and *password*, the **Status** for the unit will be listed as **Bad** logon and you will be prompted to enter the correct information when you add the unit. If you want to use the same username and password for all the cameras on your system, select the **Save** as default authentication for all manufacturers' option.

You can also add a unit manually, by clicking the **Manual add** button at the bottom of the **Unit enrollment** tool dialog box.

- **NOTE:** For video units, if the added camera is an encoder with multiple streams available, each stream is added with the *Camera - n* string appended to the camera name, *n* representing the stream number. For an IP camera with only one stream available, the camera name is not modified.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 370 of 430

3.14.2.4 Clear an Added Unit

You can clear units that have already been added to your system, so they are not displayed every time you use the **Unit enrollment** tool to discover units on your system.

The **Clear completed** option in the **Unit enrollment** tool is permanent, it cannot be reversed.

To Clear Added Units:

1. Add the desired discovered units to your system.
2. Once the units have been added, click **Clear completed**.

Any unit that has **Added** displayed in the **Status** column will be cleared from the list of discovered units.

3.14.2.5 Ignore Units

You can choose to ignore units so they don't appear in the list of discovered units of the **Unit enrollment** tool.

To Ignore a Unit:

1. From the home page, click **Tools > Unit enrollment**. The **Unit enrollment** tool opens with the list of units that have been discovered on the system.
2. **Right-click** the unit you want to ignore and select **Ignore**. The unit is removed from the list and will be ignored when the **Unit enrollment** tool discovers new units.

3.14.2.6 Remove Units from List of Ignored Units

You can remove a unit from the list of ignored units so it's not ignored when a discovery is performed by the Unit enrollment tool.

To remove a unit from the list of ignored units:

1. From the **home** page, click **Tools > Unit enrollment**.
2. In the upper right corner of the **Unit enrollment** dialog box, click **Settings and Manufacturers** (⚙).
3. Click **Ignored units** and click **Remove all ignored units**, or you can select a single unit and click the **Remove ignored unit** button (✖).

3.14.3 Unit Replacement Tool

Unit replacement is a tool that is used to replace a failed hardware device with a compatible one, while ensuring that the data associated to the old unit gets transferred to the new one. For an access control unit, the configuration of the old unit is copied to the new unit. For a video unit, the video archive associated to the old unit is now associated to the new unit, but the unit configuration is not copied.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 371 of 430

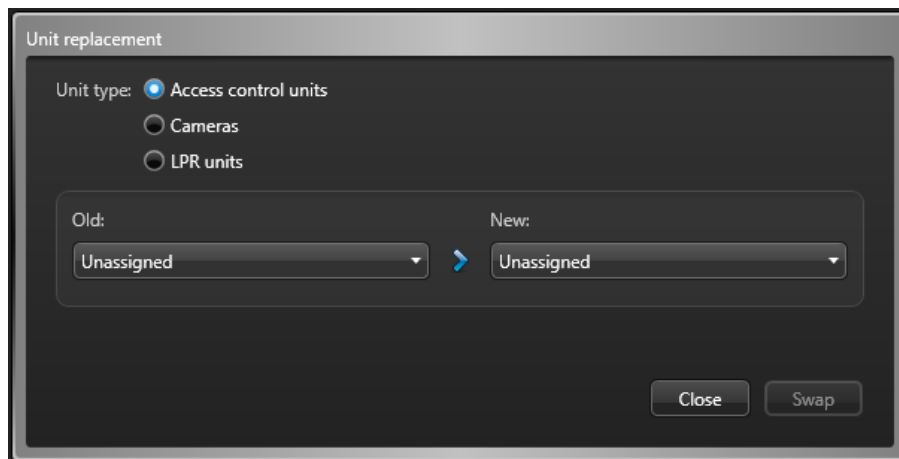


Figure 215. Security Center Tools: Unit Replacement Tool

E. Click **Swap**.

The video archives and event logs associated to the old cameras are now associated to the new cameras.

3. If the old cameras were associated with entities such as doors and alarms, represented on maps, or used for visual tracking, you must manually replace these associations.

3.14.3.1 Prepare to Replace an Access Control Unit

Before you replace an access control unit with a new one, there are steps you must perform first. You can only replace an access control unit with a new one if the two are of the same brand and model.

The only exception to this rule is if you are replacing an *HID VertX V1000* unit with a *Synergis™* unit. In every case, the exact same interface modules (brand and model) must be attached to the new unit. If there is any difference other than the above mentioned exception, the unit replacement will not be accepted.

Before you replace an access control unit:

1. Backup the **Directory** database from **Server Admin**.
2. Physically disconnect the old unit, and make sure it is offline in *Security Center* ().
3. (*Synergis™* unit only) Assemble and install the *Synergis™* unit and its hardware components. For information, see the *Synergis™ Cloud Link Hardware Installation Guide*.
4. Physically disconnect the interface modules from the old unit and connect them to the new unit using the exact same channels.
 - **IMPORTANT:** Do not change the physical address of the interface modules.
 - If you are replacing an *HID VertX V1000* unit with a *Synergis™* unit, connect the subpanels (interface modules) found on each side of the V1000 to two different channels of the *Synergis™* unit, for two interface modules on the same channel cannot have the same physical address.
5. (*Synergis™* unit only) *Configure the Synergis™* unit according to the interface modules attached to it. For more information, see the *Synergis™ Appliance Configuration Guide*.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 372 of 430

6. After you finish Replace the old unit with the new one.

3.14.4 Replace Access Control Units

If an access control unit fails and is offline in *Security Center* (🔴), you can replace the unit with a compatible one. This process copies the configuration settings, associations to doors, zones and event logs from the old unit, so you do not have to configure the new one.

Prepare to replace your access control unit.

CAUTION: Not all settings are copied by the Unit replacement tool. If you were using supervised inputs on the old unit, you will have to reconfigure the inputs on the new unit.

To replace an access control unit:

1. Add the fully wired new access control unit to the **Access Manager** controlling the old unit. For a *Synergis™* unit, see the *Synergis™ Appliance Configuration Guide*.
2. Temporarily deactivate the **Access Manager**.
 - A. In the **Access control** task, select the **Access Manager**, and click **Maintenance > Deactivate** role (🔴).
 - B. In the confirmation dialog box that opens, click **Continue**.

The **Access Manager** and all the access control units controlled by the role turn red.

3. Click the **home** page, click **Tools > Unit replacement**.
4. In the **Unit type** option, select **Access control units**.
5. Select the **Old** and the **New** access control units.
6. Click **Swap**.

(V1000 to *Synergis™* only) If the V1000 had subpanels (interface modules) using the same physical address, link the V1000 sides to the *Synergis™* unit channels, and click Continue.

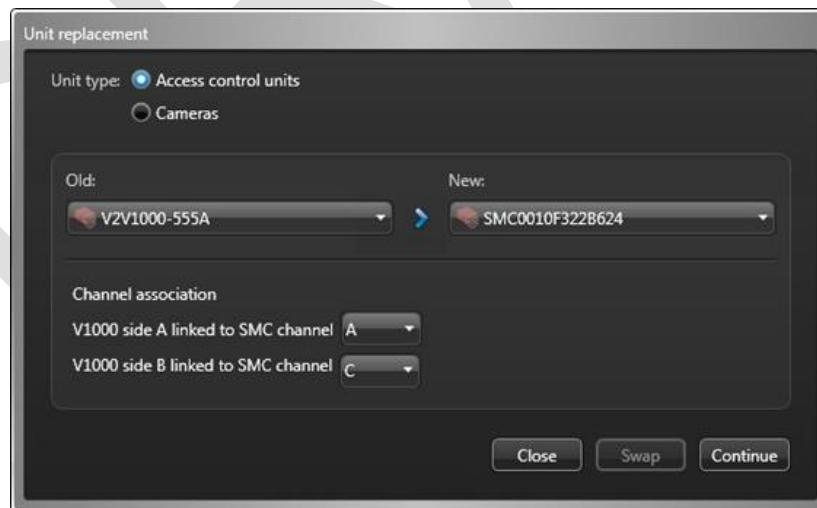


Figure 216. Security Center Tools: Unit Replacement

The configuration settings of the old access control unit are copied to the new one.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 373 of 430

7. In the **Access control** task, right-click the **Access Manager**, and click **Maintenance > Activate** role ().
8. In the **Roles and units** view, select the new unit, and verify that the configuration settings are all correct.
9. **Right-click** the old unit and click **Delete** (X).
10. In the **confirmation** dialog box that opens, click **Continue**.
11. After you finish, if the inputs on the old unit were supervised, reconfigure them on the new unit.

3.14.5 Move Unit Tool

Move unit tool is used to move units from one manager role to another. The move preserves all unit configurations and data. After the move, the new manager immediately takes on the command and control function of the unit, while the old manager continues to manage the unit data collected before the move.

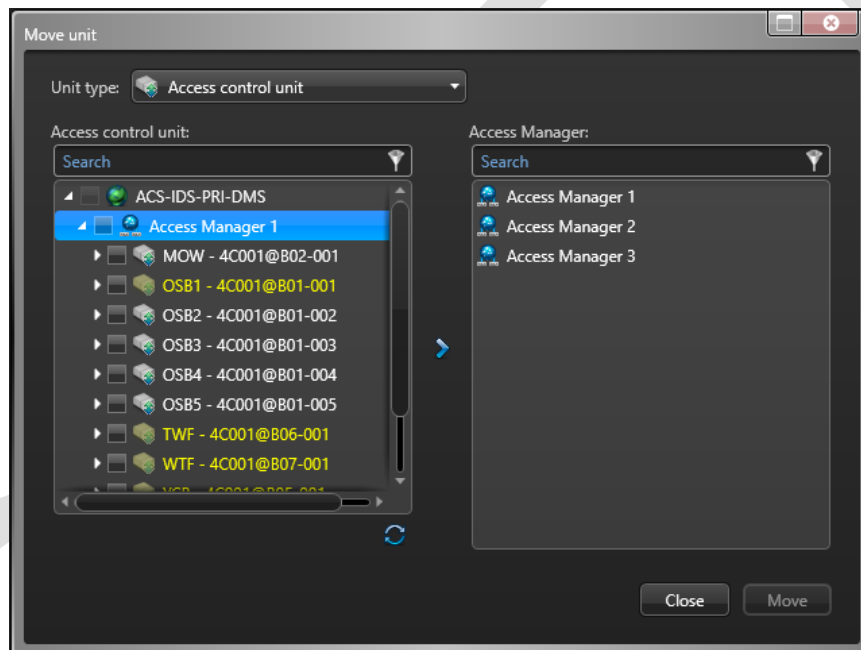


Figure 217. Security Center Tools: Move Unit Tool

3.14.5.1 Moving Video Units to a Different Archiver

If you want a different **Archiver** role to manage and control a video unit, for load distribution or another purpose, you can move the unit to another **Archiver** using the **Move unit** tool.

- The Archiver role must be on the same *LAN* as the video unit it controls.
- If you are using custom settings for the unit extension, such as custom logon credentials, you must configure the same extension settings on the new **Archiver** role.

Existing archives are not moved with the video unit to the new Archiver role. They remain associated with the old Archiver until their retention period ends.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 374 of 430

To move a video unit to a different Archiver:

1. From the **Config Tool** home page, click **Tools > Move unit**.
2. From the **Unit type** drop-down list, select **Video unit**.
3. Select the units you want to move.
4. Under **Archiver**, select the new **Archiver** role to control the unit.
5. Click **Move > Close**.
6. After you finish, move any important video archives over to the new **Archiver** at a convenient time.

3.14.5.2 Moving Intrusion Detection Units to a Different Intrusion Manager

If you want a different **Intrusion Manager** role to manage and control an intrusion detection unit, for load balancing or another purpose, you can move the unit to another **Intrusion Manager** using the **Move unit tool**.

- The **Intrusion Manager** role must be on the same *LAN* as the intrusion detection unit it controls.
- If the unit extension is not created automatically, you must add it.
- If the intrusion panel is physically connected to a serial port on the server hosting the original role, make sure you do the same with the server hosting the new role.

To move an intrusion detection unit to a different Intrusion Manager:

1. From the **home** page, click **Tools > Move unit**.
2. From the **Unit type** drop-down list, select **Intrusion detection unit**.
3. Select the units you want to move.
4. Under **Intrusion Manager**, select the new **Intrusion Manager** role to control the unit.
5. Click **Move > Close**.

3.14.6 Copy Config Tool

The **Copy configuration** tool helps you save configuration time by copying the settings of one entity to many others that partially share the same settings.

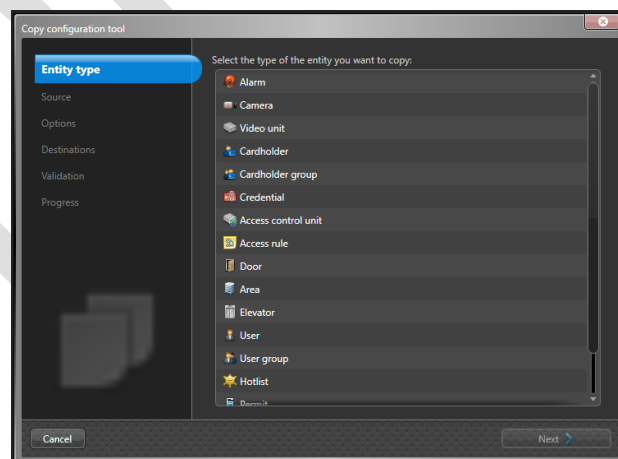


Figure 218. Security Center Tools: Copy Config Tool

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 375 of 430

3.14.6.1 Copying Configuration Settings from One Entity to Another

When you have many similar entities to configure, you can save time by copying the settings of one entity to others of the same type using the **Copy configuration** tool. If you are copying camera settings, make sure the cameras are the same brand and model so the settings match.

(Cameras only) If you are copying the camera's network settings, only the streaming settings are copied (Connection type and UDP port). The **Multicast** address is not copied.

To copy the configuration settings of one entity to another entity:

1. Open the **Copy configuration** tool one of the following ways:
 - From the **Config Tool** home page, click **Tools > Copy** configuration tool.
 - From the **Config Tool**, **right-click** an entity in any entity tree, and then click **Copy > Copy** configuration tool.
2. If you opened the **Copy configuration** tool from the home page, then select an entity type, and click **Next**.
3. In the **Source** page, select which entity you want to copy the settings from, and click **Next**.
4. In the **Options** page, select the types of settings you want to copy, and click **Next**. To know which options are available for each entity, see the following list.
5. In the **Destinations** page, select the entities you want to copy the settings to, and click **Next**.
6. When the copying process is completed, click **Close**.

After you finish

If you copied camera settings, test the settings that are dependent on camera location (for example, motion detection or color) on the camera you copied the configuration to. You might have to adjust the settings, depending on whether the camera is inside or outside, in a busy or quiet location, and so on.

3.14.6.2 Settings Copied for Each Entity Using the Copy Configuration Tool

You can determine which categories of settings are copied when using the **Copy Configuration** tool. The available categories are different for each entity.

[Table 39](#) lists the categories of settings that are available for each entity when using the **Copy Configuration** tool.

Table 39. Security Center Tools: Copy Configuration Tool: Entities Setting Categories

Entity Type	Setting Categories Available
Access Control unit	• Actions • Properties (HID only) — All settings in the Properties tab, except the ones covered under the Security category. • Security (HID only) — Includes: Secure mode and Admin password. • Synchronization • Time Zone
Access rule	• Attached entities

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 376 of 430

Entity Type	Setting Categories Available
	- Members - Properties
Alarm	- Actions - Attached entities - Properties - Recipients
Area	Maps
Camera	- Actions - Boost quality - Color - Encryption - Hardware specific settings - Motion detection - Network - PTZ - Recording - Stream usage - Video quality - Visual tracking
Cardholder	- Access rules - Actions - Options - Parent cardholder groups - State
Cardholder group	- Access rules - Members - Parent cardholder groups - Properties
Credential	- Actions - Badge template - State
Door	- Access rules - Actions - Cameras - Properties - Unlock schedules
Hotlist	- Advanced - Attributes - Path

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 377 of 430

Entity Type	Setting Categories Available
	Properties
User	- Access rights - Actions - Advanced - Alarms - Privileges - Properties - Security Desk settings
User group	- Access rights - Advanced - Alarms - Members - Privileges - Properties - Security Desk settings
Video unit	- Actions - Audio - Hardware specific settings - Motion detection - Network - Security - Time Zone
Zone	Actions

3.14.7 Upgrade Firmware

In computing, firmware is a specific class of computer software that provides the low-level control for a device's specific hardware.

A firmware upgrade is a software program that can be used to update the firmware in hardware devices. For example, a user could download a firmware update for a network router that enhances its capabilities or fixes an issue. Firmware updates are generally available from hardware manufacturers.

3.14.7.1 Upgrading Video Unit Firmware

You can upgrade the firmware on your video unit directly from **Config Tool**.

If *Genetec™ Update Service* is running, the status of the firmware upgrade is indicated in the unit's Identity page and in the Proposed firmware description column of the **Hardware inventory** report:

- **Up to date:** No firmware upgrade is necessary.
- **Optional:** The firmware upgrade is suggested.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 378 of 430

- **Recommended:** The firmware upgrade is recommended.
- **Critical:** The firmware upgrade fixes a security vulnerability issue and is highly recommended.
 - Download the recommended firmware from the manufacturer's website. If *GUS* is not running, you can find the recommended firmware for your unit from our *Supported Device List*.
 - Take note of the unit's configuration settings. For some manufacturers, the unit is reset to its default settings after the firmware upgrade.

For some manufacturers, you cannot upgrade the unit's firmware from **Config Tool**. For manufacturer- specific information, see the manufacturer's documentation.

To upgrade a video unit's firmware:

1. From the **Config Tool** home page, open the **Video** task.
2. Select the video unit to upgrade, and click the **Identity** tab.
3. Click **Upgrade** (🔧).
4. In the **Upgrade firmware** dialog box, browse to the firmware file that you downloaded and click Upgrade.

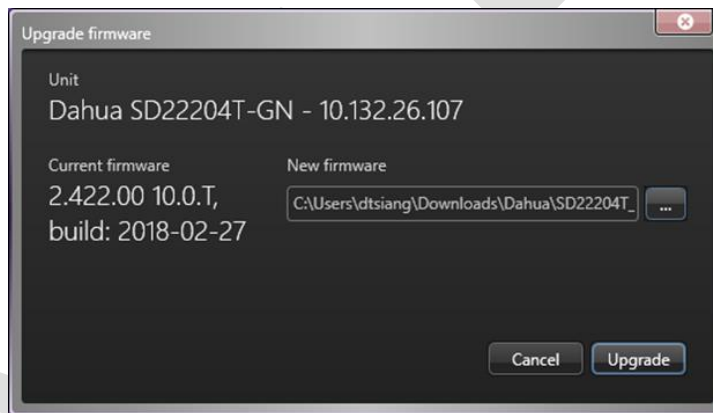


Figure 219. Upgrade Firmware

5. The unit restarts.
6. After you finish reconfigure the unit if it was reset to default settings during the upgrade.

3.14.7.2 Upgrade Access Control Unit Firmware

You can upgrade the firmware of one or more access control units and their connected interface modules directly from Config Tool.

- If the units are powered by Power over Ethernet (PoE), they should include a battery backup in case of a power failure during the upgrade process.
- Download a supported firmware version for the unit from GTAP.
 - **NOTE:** For HID EVO firmware download links, see KBA01134 on the *Genetec™ TechDoc Hub*.
- For HID EVO units, ensure that the admin password is set in **Config Tool** under the unit's properties.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 379 of 430

- You can upgrade the following devices from **Config Tool**:
 - Synergis™* Cloud Link
 - Synergis™* Master Controller
 - Supported upgrade path: 2.x → 10.0 → any later version
 - Mercury EP (when connected to a *Synergis™ Cloud Link* or *Synergis™* Master Controller running *Synergis™ Softwire* 10.4 or later.)
 - Axis A1001 (when connected to a *Synergis™ Cloud Link* or *Synergis™* Master Controller running *Synergis™ Softwire* 10.4 or later.)
 - Assa Abloy IP locks (when connected to a *Synergis™* Cloud Link or *Synergis™* Master Controller running *Synergis™ Softwire* 10.5 or later.)
- To upgrade HID EVO units from an earlier firmware version (2.3.1.603 or 2.3.1.605 for Edge EVO, and 2.3.1.542 or 2.3.1.673 for VertX EVO) to the recommended firmware version, specific upgrade paths must be followed:
 - HID Edge EVO: (EH400, EH400-K)
 - Supported upgrade path: 2.3.1.603 or 2.3.1.605 → 2.3.1.841 → any later version
 - HID Vertx EVO: (V1000, V2000)
 - Supported upgrade path: 2.3.1.542 or 2.3.1.673 → 2.3.1.791 → any later version
 - CAUTION:** Upgrading directly from the earlier firmware to the recommended firmware will cause irreparable damage to your unit. Moreover, you cannot downgrade the firmware after it has been upgraded to 2.3.1.841 on Edge EVO or to 2.3.1.791 on VertX EVO.
- Individual units can also be upgraded in the **Access control** task in **Config Tool** from the unit's Identity tab in the Roles and units view.
- The system can upgrade up to ten units concurrently. If more than ten units are selected for upgrade, additional units are queued.
- You cannot cancel an upgrade that is in progress. You can only cancel an upgrade if the unit's upgrade status in the **Hardware inventory** report is scheduled.
- Doors assigned to the access control unit being upgraded do not function during a firmware upgrade.

To upgrade access control unit firmware:

- In **Config Tool**, generate a Hardware inventory report for the units you want to upgrade.
- Select the units that you want to upgrade.

The **Proposed** field displays the recommended firmware version. If the firmware version is the same as the proposed version, it will display **Up to date**.

NOTE: If you select multiple units to upgrade, all of the selected units must be of the same product type.

- Click **Upgrade firmware** (🔧).

NOTE: If the Upgrade firmware button does not appear, make sure that you have the required user privileges (requires the Initiate access control unit firmware upgrade privilege and the **Unit discovery** tool privilege), and make sure that all of the selected units are of the same product type.

- In the file browser, select the firmware file that you downloaded from *GTAP*, and click **Open**.
- To upgrade the firmware of interface modules connected to the controller, select **Upgrade the**

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 380 of 430

firmware of connected interface modules.

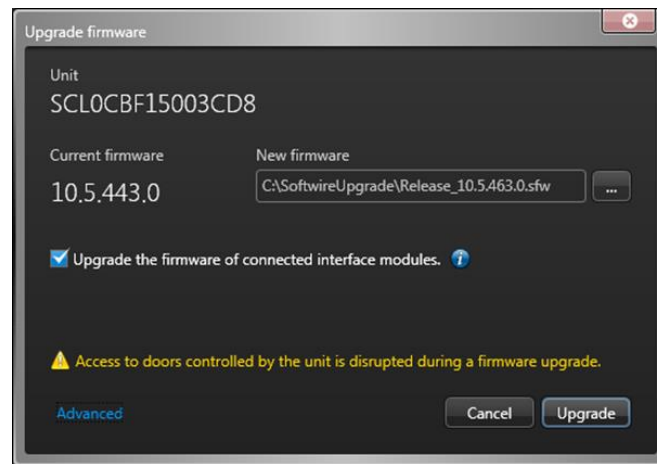


Figure 220. Upgrade Firmware

- **NOTE:** It is recommended that you select this setting when upgrading HID Edge EVO or HID VertX EVO V2000 controllers. This setting is optional for VertX EVO V1000 (up to 3 minutes per interface), Synergis™ Cloud Link, and Synergis™ Master Controller units.
6. To delay the upgrade, click **Advanced**, select **Delay upgrade until**, and define the upgrade date and time.

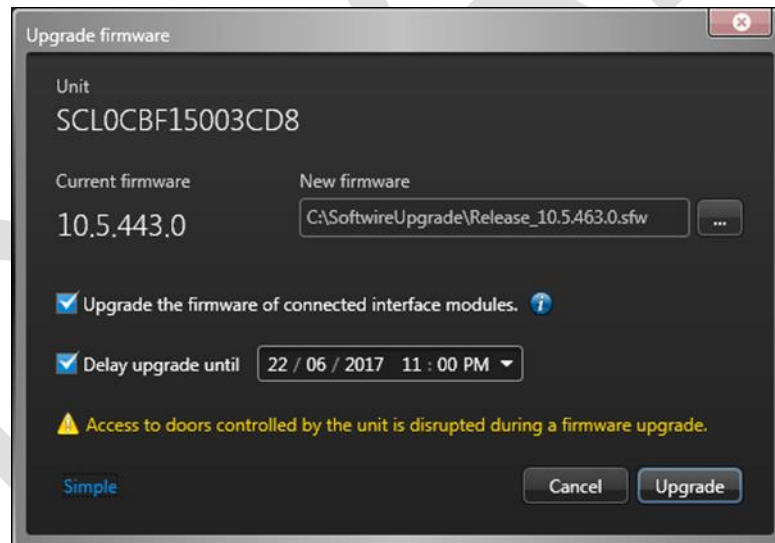


Figure 221. Upgrade Firmware: Delay Upgrade

7. Click **Upgrade**. The system upgrades the access control units' firmware and the units restart.
8. After you finish, when the units come back online, generate another Hardware inventory report in Config Tool and confirm the firmware version displayed for the units.
- **NOTE:** For HID EVO units, if Upgrade the firmware of connected interface modules was selected, the unit stays offline until the interface module firmware upgrade is completed.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 381 of 430

- Verify that all doors controlled by the upgraded units are operating properly.

3.15 REPORTS

At this time, management has not required delivery of specific operational logs or reports. However, [Table 40](#) provides a list of reports that Genetec operators can create.

Table 40. Genetec Security Desk – Types of Reports Available

#	Type of Report	Name of Report	Description
1	Administrative	Incident Configuration Report	• Generate reports on the changes made to incident types
2	Administrative	Intrusion Manager Report	• Provides live reports to Security Center, and logs the events in a database for future reporting.
3	Investigation	Door Activities Report	• Reports on door related activities, such as access denied, door forced open, door open too long, hardware tamper, etc.
4	Investigation	Cardholder Activities Report	• Investigate events related to cardholders, such as Access denied: Invalid PIN , First person in, Last person out, Antipassback violation, etc.
5	Investigation	Alarm Report	• Allows you to search and view current and past alarms
6	Investigation	Archive Report	• List of available video archives on the system by camera and time range
7	Investigation	Area Presence Report	• View the number of cardholders and visitors currently present in a selected area and how long they have been there
8	Investigation	Bookmark Report	• List of all the stored bookmarks
9	Investigation	Camera Events Report	• Reports on events pertaining to selected cameras within a specified time range
10	Investigation	Credential Activities Report	• Reports on credential related activities, such as access denied due to expired, inactive, lost, or stolen credential, etc.
11	Investigation	Cardholder Time and Attendance Report	• Research which cardholders have been inside a selected area and the total duration of their stay within a given date range
12	Investigation	Credential Request History Report	• Reports on which users requested, cancelled, or printed cardholder credentials.
13	Investigation	Elevator Activities Report	• Reports on elevator related activities, such as access denied, floor accessed, unit is offline, hardware tamper, and so on.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 382 of 430

Table 40. Genetec Security Desk – Types of Reports Available

#	Type of Report	Name of Report	Description
14	Investigation	Enhanced Cardholder Access Rights Report	Investigate which cardholders and cardholder groups are currently granted or denied access to selected areas, doors, and elevators, etc.
15	Investigation	Forensic Search Report	Search for video analytics events recorded on Bosch units
16	Investigation	Incident Report	An unexpected event reported by a Security Desk user; they can use formatted text and include events and entities as support material.
17	Investigation	Intrusion Detection Area Activities Report	A type of investigation reports on activities (master arm, perimeter arm, duress, input trouble, and so on) in selected intrusion detection areas.
18	Investigation	Intrusion Detection Unit Event Report	Reports on events (AC fail, battery fail, unit lost, input trouble, and so on) related to selected intrusion detection units.
19	Investigation	Inventory Report	Report for specific inventory (vehicle location, vehicle length of stay, etc.) or to compare two inventories of a selected parking facility (e.g., vehicles added, vehicles removed, etc.)
20	Investigation	Motion Search Report	Search video archives for video sequences that detect motion in specific areas of a camera's field of view
21	Investigation	Time and Attendance Report	Reports on who has been inside a selected area and the total duration of their stay within a given time range.
22	Investigation	Visitor Activities Report	Report events related to visitors (access denied, first person in, last person out, antipassback violation, etc.
23	Investigation	Visit Details Report	Reports on the stay (check-in and check-out time) of current and past visitors.
24	Investigation	Zone Activity Report	Report on zone related activities (zone armed, zone disarmed, lock released, lock secured, etc.
25	Investigation	Zone Occupancy	Report on the number of vehicles parked in a selected parking area, and the percentage of occupancy.
26	Maintenance	Access Control Health History Report	Reports on malfunction events for access control units
27	Maintenance	Access Control Unit Event Report	Reports on events pertaining to selected access control units

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 383 of 430

Table 40. Genetec Security Desk – Types of Reports Available

#	Type of Report	Name of Report	Description
28	Maintenance	Access Rule Configuration Report	Reports on entities and access points affected by a given access rule.
29	Maintenance	Activity Trails Report	Reports on the user activity related to video, access control. It provide information such as who played back which video recordings, who used the Hotlist permit editor, who enabled hotlist filtering, etc.
30	Maintenance	Archiver Events Report	Reports on events pertaining to selected Archiver roles
31	Maintenance	Archive Storage Details Report	Reports on the video files (file name, start and end time, file size, protection status, and so on) used to store video archive, and which allows you to change the protection status of those files, etc.
32	Maintenance	Camera Configuration Report	Reports on the properties and settings of local cameras in the system (manufacturer, resolution, frame rate, stream usage, etc.)
33	Maintenance	Cardholder Access Rights Report	A type of maintenance task that reports on which cardholders and cardholder groups
34	Maintenance	Cardholder Configuration Report	Reports on cardholder properties, such as first name, last name, picture, status, custom properties, etc.
35	Maintenance	Hardware Inventory Report	Reports on the characteristics such as unit model, firmware version, IP address, time zone, and so on) of access control, video, and intrusion detection units, etc., in the system.
36	Maintenance	Health History Report	Reports on system health issues
37	Maintenance	I/O Configuration Report	Report on the I/O configurations (controlled access points, doors, and elevators) of access control units

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 384 of 430

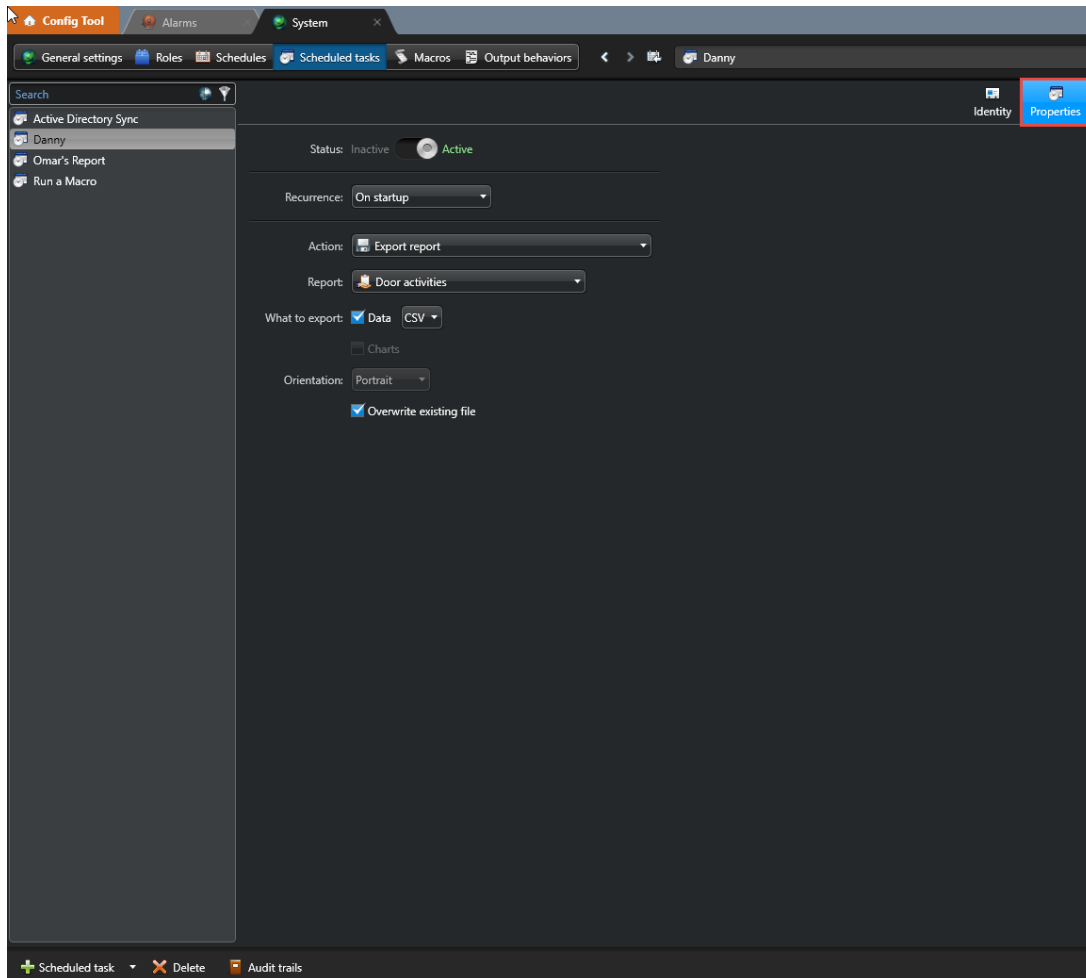


Figure 222. Scheduled Tasks: Properties: Schedule Routine Reports

3.15.1 Schedule Routine Reports

You can schedule Genetec Security Desk to automatically create a report and email it to someone on a regular basis, whether it's daily, weekly, monthly, or annually. The following Genetec reports are typical examples of routine reports you can provide to management upon their request or for regular receipt.

- Hardware Configuration Report
- Door Activities Report
- Cardholder Activities Report

3.15.1.1 Hardware Inventory Report

To Generate a Hardware Inventory Report:

1. Using either the Security Desk or the Config Tool, open a new **Hardware Inventory Task** (Maintenance).

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 385 of 430

In the query filters pane on the left side, turn off the **Units** filter and turn off the **Source group** filter. Click **Generate Report**.

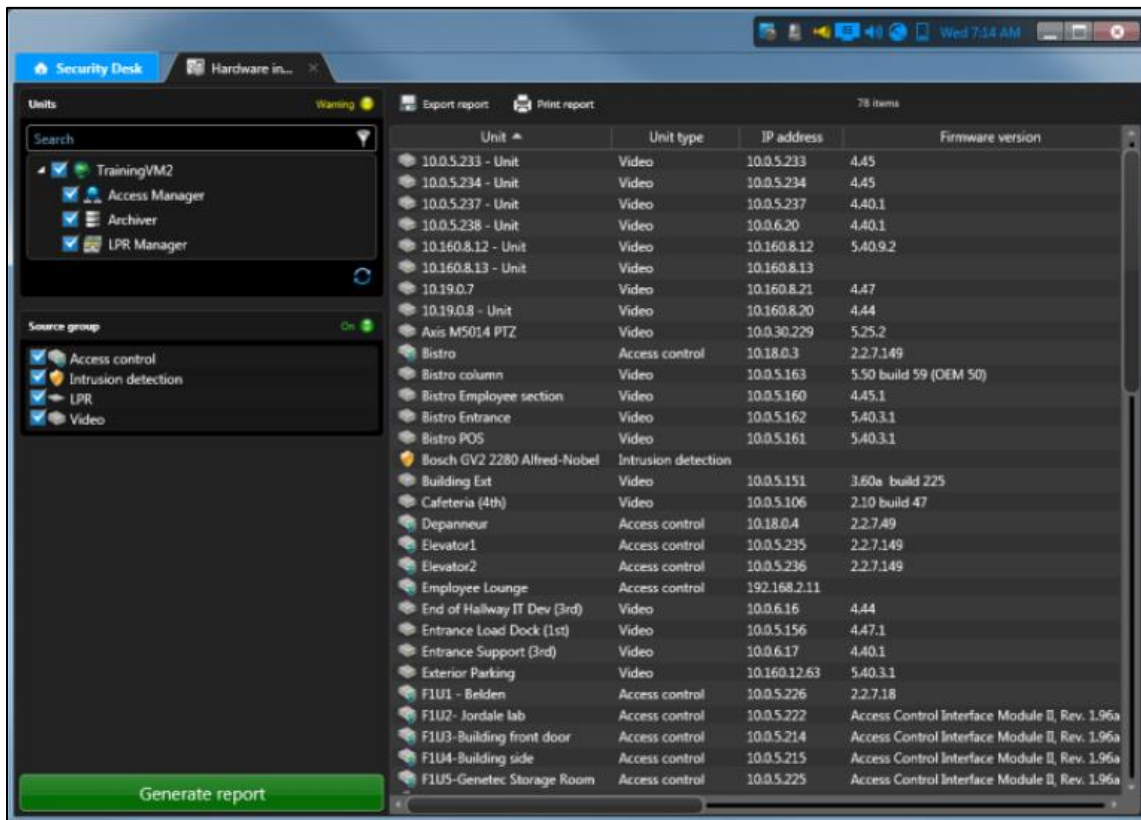


Figure 223. Security Center Troubleshooting – Hardware Inventory Report

Click **Export report**. Save your inventory report as a Microsoft Excel file.

In the query filters pane on the left side, turn on the **Units** filter and turn on the **Source group** filter. Try different combinations of query filters.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 386 of 430	

3.15.1.2 Door Activities Report

You can investigate events related to doors (Door forced open, Door open too long, Hardware tamper, and so on), using the **Door activities report**.

To Investigate Door Events and Create a Door Report:

1. From the home page, open the **Door activities** task.
2. Set up the query filters for your report. Choose one or more of the following filters:
 - **Cardholders:** Restrict the search to certain cardholders.
 - **Credentials:** Restrict the search to specific credentials.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
 - **Doors:** Select the doors to investigate.
 - **Events:** Select the events of interest. The event types available depend on the task you are using.
 - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the previous week or the previous month.
3. Click **Generate report**. The door events are listed in the report pane.
4. To show the corresponding video of an event in a tile, double-click or drag the item from the report pane to the canvas. If there is no camera attached to the door, the door icon is displayed.
5. To control the doors, use the door widget.
 - **Example:** You can see how many access denied events have occurred in the last week, or since your last shift, or search for other critical events (For example, Door forced open). If you see suspicious cardholder activity while monitoring live video, you can investigate what other doors the cardholder accessed in the last day. If you want to see if the maintenance staff has completed work at a particular door, you can investigate on that door, and select the Door maintenance completed event.

Report Pane Columns for the Door Activities Task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **NOTE:** If you generated the Door activities report using Web Client, not all of the report columns are available.
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Door:** Door name.
- **Email address:** Cardholder or visitor's email address.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 387 of 430

- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder or visitor's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Side:** Door side name.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, or intrusion detection unit involved.

3.15.1.3 Cardholder Activities Report

You can investigate events related to cardholders (Access denied: Invalid PIN, First person in, Last person out, Antipassback violation, and so on), using the Cardholder activities report. For example, if you want to see which areas, doors, and elevators the cardholder has access in the last day or week, you can search for that specific cardholder, and set a time range for your report. If there has been suspicious activity on your site in the last day, you can investigate which cardholders were denied access to an area by selecting the area, and the Access denied event.

To Investigate Cardholder Events:

1. From the home page, open the Cardholder activities task.
2. Set up the query filters for the report. Choose from one or more of the following filters:
 - **Cardholders:** Restrict the search to certain cardholders.
 - **NOTE:** If you only select the All cardholders cardholder group, federated cardholders are not included. This is because All cardholders is a local cardholder group that only covers local cardholders.
 - **Credentials:** Restrict the search to specific credentials.
 - **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
 - **Doors - Areas - Elevators:** Restrict the search to activities that took place at certain doors, areas, and elevators.
 - **Events:** Select the events of interest. The event types available depend on the task you are using.
 - **Event timestamp:** Define the time range for the query. The range can be defined for a specific period of time or for global units of time such as the previous week or the previous month.
3. Click **Generate report**. The cardholder events are listed in the report pane.
4. Show the corresponding video of an event in a tile by double-clicking or dragging the item from the report pane to the canvas. If there is no camera attached to the entity, the door, elevator, or area icon is displayed, depending on the type of cardholder event.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 388 of 430

5. Control the tiles using widgets in the dashboard.

Report Pane Columns for the Cardholder Activities Task

After generating a report, the results of your query are listed in the report pane. This section lists the columns available for the relevant reporting task.

- **Access point:** Access point involved (only applicable to areas, doors, and elevators).
- **Card format:** Credential card format.
- **Cardholder:** Cardholder entity name.
- **Credential:** Credential name used by the cardholder.
- **Credential code:** Facility code and card number.
- **Custom fields:** The pre-defined custom fields for the entity. The columns only appear if custom fields are defined for the entity, and if the custom fields were made visible to you when they were created or last configured.
- **Device:** Device involved on the unit (reader, REX input, IO module, Strike relay, etc.).
- **Email address:** Cardholder or visitor's email address.
- **Event:** Event name.
- **Event timestamp:** Date and time that the event occurred.
- **First name:** Cardholder or visitor's first name.
- **IP address:** IP address of the unit or computer that generated the event.
- **Last name:** Cardholder or visitor's last name.
- **Location:** Location (area) where the activity took place.
- **Occurrence period:** Period when the event occurred.
- **Picture:** Cardholder or visitor's picture.
- **Product type:** Model of the unit involved.
- **Supplemental credential:** A second credential is sometimes necessary. For example, when both a card and a PIN are required to access a door or elevator.
- **Time zone:** Time zone of the unit.
- **Unit:** Access control, video, or intrusion detection unit involved.

3.16 NORMAL OPERATIONS

Normal operations are defined as all relevant equipment and infrastructure provided specifically for HART that are working normally as designed and fulfilling the operational requirements with no failure, natural hazard, or any other outside failure occurring. The content of this manual assumes all operations occur in normal daily functions.

3.17 DEGRADED OPERATIONS

A degraded operation is a situation in which a failure of equipment/infrastructure or an incident has occurred, but a part of the operations can continue, though with some operational restrictions. Degraded operations do not usually involve life threatening situations nor result in serious injuries or damage to properties.

A degraded operation means there is an implementation of a temporary workaround usually in the form of manual or alternative services to implement to maintain minimum services during equipment

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 389 of 430

failures or operational incidents. The objective of degraded operation is to maintain an optimal level of service that can be delivered within the constraints of situation.

When the operator first notices an inability to use a function or tool, the first step is to troubleshoot it and bring it back online as efficiently as possible. The following scenarios describe possible degraded conditions and procedures to correct the issues before they worsen.

3.17.1 Cloud Link is Working but Server is Down

3.17.2 Inability to View System Messages

The inability to view system messages in Security Center is a degraded operation because the operator's response time to attend to the message is affected.

To View System Messages:

- Health issues**

 - From the **Sort by** dropdown list, select how to display the health issues. You can sort them alphabetically by health event type, event timestamp, machine (computer name), or source (entity name).
 - Click an entity to open its configuration pages, to diagnose the entity. You must have access to Config Tool.
 - Click  in a row to launch a **Health history** task and view system health events.
 - Click **Refresh** to update the content displayed in the **Health issues** tab.

System messages 

Notifications

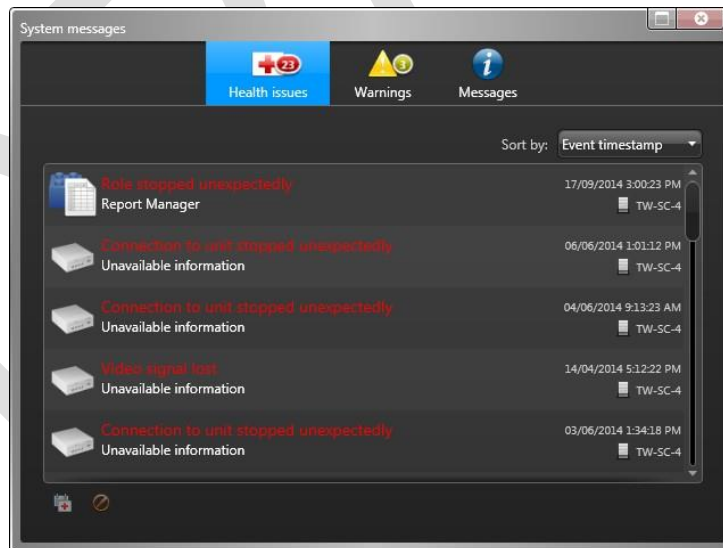


Figure 224. Genetec Security Desk – View System Messages

Warnings

- Click an entity to open its configuration pages. You can only jump to the entity's configuration pages if you have access to Config Tool.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 390 of 430

- Click **Details**  to open the diagnostic window, which provides additional details about the warning.
- From this window you can save the warning as a text file; or click **Refresh** to rerun the diagnostic tests.

Messages

- Click **Copy to clipboard** to copy the selected message to the clipboard.
- Click **Clear all** to delete the selected messages.
- Click **Clear all** to clear all messages.

**Notifications**

3.17.3 Inability to View Availability of Entities

The inability to view system health status and the availability of entities may be considered a degraded operation because the operator's ability to confirm the system health and status of an entity (such as a camera, door, alarm, user, role, plugin, etc.) is delayed.

To View the Availability of an Entity:**Health statistics**

- **Custom fields:** Restrict the search to a pre-defined custom field for the entity. This filter only appears if custom fields are defined for the entity, and if the custom field was made visible to you when it was created or last configured.
- **Event timestamp:** Define the time range for the query. The range can be defined for a specific period or for global units of time such as the previous week or the previous month.
- **Source entity:** Source entity of the event.
- **Source group:** Source entity group of the event. Usually a role or a unit.

Generate report

- The health statistics for the selected entities are listed in the report pane. If health statistics could not be calculated for a given role or entity, the reason is shown in the Calculation status column of the report pane:
- One or more events used to calculate availability are currently disabled: The system administrator needs to select which health events to monitor by configuring the Health monitor role.
- One or more servers from the system are offline: The server hosting the selected role is offline, therefore, the health statistics cannot be calculated for the role.
- **Example:** A door controller called Gym was down four times over the last week, producing 90.72% availability. From the report results, you can see that this door controller is a potential concern and have a maintenance crew come and look at the door.

3.17.4 SQL Server/Database Failure

If the SQL Server/database experiences a partial or full failure, Security Center will failover to the SQL Server/database in the BOCC. Security Center would continue to run with a degraded performance due to the network latency between OCC and BOCC sites.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 391 of 430

3.17.5 Workstation Failure

The OCC has nine workstations that perform the following functions:

- One Supervisor - Fault management/reporting
- Two Call Takers - Fault management/reporting and operations control
- Two Rail Operator Controllers - Fault management/reporting
- Two Security/CCTV Operators - Fault management/reporting and operations control
- Two Yard Operators - Fault management/reporting

If one workstation experiences a power disruption it is degraded; the operator should move to a workstation in the BOCC.

To prevent a non-emergency disruption of power (for example, an error message of not enough disc space to run the system programs), an operator should perform routine workstation maintenance per the vendor recommendations.

3.17.6 Monitor Failure

In the event of a temporary power loss to one monitor, a redundant workstation already provides the same function so there is essentially no down time that affects the system. For example:

- There are two OCC workstations for call takers, each workstation has three monitors designated for telecom equipment.
- There are two OCC workstations for rail operator controllers, each workstation has one monitor designated for telecom equipment.
- There are two OCC security/CCTV operators, each workstation has two monitors designated for security equipment. This station also has its own small video wall with four simultaneous video viewing areas.
- There are two OCC yard operators, each workstation has one monitor designated for telecom equipment.
- The supervisor also has a workstation with one monitor designated for telecom equipment.

In the event one monitor experiences an interruption in power, this would be a degraded operational scenario. It is not an emergency because another monitor is already in use is continuing to view the same areas.

However, if a monitor on two or more workstations experience a power loss, this is a degraded situation because there is a lack of consistent viewing of all areas. If this occurs, the operators of the affected workstations should immediately move to workstations in the BOCC. Operators should not remove the monitors from the BOCC at any time. Once the monitor is replaced in the OCC and full workstation functionality is confirmed, then the operator may return to the original OCC workstation.

3.17.7 HART Switchover from OCC to BOCC

A degraded operation for CCTV is the switchover of operations from OCC to BOCC. Security Center is installed in the OCC and BOCC. These systems are synchronized by the Genetec Security Center Failover Service – this configuration helps to avoid a single hardware or software point of failure. If the entire CCTV system becomes unavailable at the OCC, the operation and supervision of HRTS is transferred to the BOCC. The running status of all the servers in OCC and BOCC are monitored by

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 392 of 430

the ICCS GSC area view.

3.18 EMERGENCY OPERATIONS

An emergency operation is an immediate emergency response to a major incident that causes serious service disruption, injuries, fatalities, or damage to the asset.

An emergency is an unplanned event, which generally has life threatening or extreme loss implications and requires immediate attention. When all scenarios of possible emergencies are considered, emphasis is placed on major incidents with emphasis on a consistent emergency response across different emergency scenarios relative to the system/subsystem.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 393 of 430	

Appendix A. Alarm List

Table A-1 is a list of alarms that Genetec receives for CCTV, ACS and IDS; the alarms appear in full text as indicated.

Table A-1. List of Genetec Alarms for ACS and IDS

#	System	Alarm Text
1	ACS	Access Denied
2	ACS	Remote Override - Unlock
3	ACS/IDS	SMC Offline!
4	ACS/IDS	Power Failure
5	ACS/IDS	Trouble Short Circuit - Input
6	ACS/IDS	Trouble Open Circuit - Input

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 394 of 430

Appendix B. Bill of Materials

Table B-1 provides the Bill of Materials (BOM) for the ACS/IDS subsystem; references are available in the following locations.

HNL Directory: 60041

Document: 3HR-79100-DJFF-BQZZA-01-HNL 60041-Communications System - CCTV Surveillance System and Security.doc

Table B-1. ACS/IDS Bill of Materials – Passenger Stations

Item	Description	Quantity	Unit
1	ACS/IDS Enclosure	4	each
1.1	Access Control Panel	4	each
1.2	Input / Output Panels	8	each
1.3	Card Reader Controller	14	each
1.3	Power Distribution Panels	8	each
1.4	Power Cable 50'	4	each
1.5	Enclosure Wiring kit	4	each
1.6	Enclosure Mounting Bracket	1	each
1.7	Terminal Blocks	16	each
1.8	DIN Rail	4	each
2	Request to Exit	14	each
3	Card Reader	14	each
4	Electric Door Strike	14	each
5	Surface Alarm Contact	14	each
6	Motion Sensor	14	each
7	Intrusion Alarm Panel/ Arming Station	1	each
8	Horn	1	each
9	Workstation	1	each
10	23" Monitor	1	each
11	110 VAC Power Cord	2	each
12	SVGA Signal Cable	1	each
13	5 Cond 18 AWG Wire	2500	ft
14	CAT6 Cable 200' (2 end RJ 45 Terminated)	2	each
15	2 Cond 18 AWG Wire	1100	ft

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 395 of 430	

Table B-2. ACS/IDS Bill of Materials – MSF Yard

Item	Description	Quantity	Unit
1	Door/Gate Interface	35	each
2	Card Reader	22	each
3	Gate Latch Strike	10	each
4	Surface Alarm Contact	42	each
5	Security Junction Box	22	each
6	5 Cond 18 AWG Wire	17500	ft
7	2 Cond 18 AWG Wire	4200	ft
8	Splice Connector, 1 Cond 18 AWG	84	each
9	Gate Controller	2	each
10	Traffic Loop, Vehicle Wheel	2	each
11	Loop Connector Cable 150'	2	each
12	Loop Detector	2	each
13	Intercom	1	each
14	Knox Box	1	each

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 396 of 430	

Table B-3. ACS/IDS Bill of Materials – OCC and OCC Equipment Room

Item	Description	Quantity	Unit
1	ACS/IDS Enclosure	1	each
1.1	Access Control Panel	1	each
1.2	Card reader Controller	16	each
1.3	Input / Output Panels	2	each
1.3	Power Distribution Panels	2	each
1.4	Power Cable 50'	1	each
1.5	Enclosure Wiring kit	1	each
1.6	Enclosure Mounting Bracket	1	each
1.7	Power Cable 50'	1	each
1.8	Terminal Blocks	4	each
1.9	DIN Rail	2	each
2	Request to Exit	16	each
3	Card Reader	16	each
4	Electric Door Strike	16	each
5	Surface Alarm Contact	16	each
6	Motion Sensor	16	each
7	Intrusion Alarm Panel/ Arming Station	1	each
7	Workstation	2	each
8	23" Monitor	4	each
9	110VAC Power Cord	6	each
10	SVGA Signal Cable	4	each
11	5 Cond 18 AWG Wire	3200	ft
12	CAT6 Cable 200' (2 end RJ 45 Terminated)	2	each
13	CAT6 Cable 50' (2 end RJ 45 Terminated)	5	each
14	2 Cond 18 AWG Wire	1100	ft

Table B4. ACS/IDS Bill of Materials – Badge Workstation Area

Item	Description	Quantity	Unit
1	Workstation w/ keyboard and mouse	1	each
2	23" Monitor	1	each
3	Power Cable	2	each
4	IP Camera	1	each
5	Badge Printer/ Encoder	1	each
6	CAT6 Cable 10' (2 End RJ 45 Terminated)	1	each
7	HID iClass or Mifare Cards	500	each

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 397 of 430

Table B5. ACS/IDS Bill of Materials – OSB Floors 1, 2 and Mezzanine

Item	Description	Quantity	Unit
1	ACS/IDS Enclosure	3	each
1.1	Access Control Panel	3	each
1.2	Card reader Controller	20	each
1.3	Input / Output Panels	6	each
1.3	Power Distribution Panels	6	each
1.4	Power Cable 50'	3	each
1.5	Enclosure Wiring Kit	3	each
1.6	Enclosure Mounting Bracket	3	each
1.7	Power Cable 50'	3	each
1.8	Terminal Blocks	12	each
1.9	DIN Rail	6	each
2	Request to Exit	20	each
3	Card Reader	20	each
4	Electric Door Strike	20	each
5	Surface Alarm Contact	20	each
6	Motion Sensor	20	each
7	Intrusion Alarm Panel/ Arming Station	20	each
7	5 Cond 18 AWG Wire	3000	ft
8	CAT6 Cable 50' (2 end RJ 45 Terminated)	1	each
9	2 Cond 18 AWG Wire	1250	ft
10	Terminal Blocks, Screw Connector	15	each
11	Splice Connector, 1 Cond 18 AWG	50	each

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 398 of 430	

Table B-6. ACS/IDS Bill of Materials – Yard Control Bungalow

Item	Description	Quantity	Unit
1	ACS/IDS Enclosure	1	each
1.1	Access Control Panel	1	each
1.2	Card reader Controller	2	each
1.3	Input / Output Panels	2	each
1.3	Power Distribution Panels	2	each
1.4	Power Cable 50'	1	each
1.5	Enclosure Wiring kit	1	each
1.6	Enclosure Mounting Bracket	1	each
1.7	Power Cable 50'	1	each
1.8	Terminal Blocks	4	each
1.9	DIN Rail	2	each
2	Request to Exit	2	each
3	Card Reader	2	each
4	Electric Door Strike	2	each
5	Surface Alarm Contact	2	each
6	Motion Sensor	2	each
7	Arming Station	1	each
8	5 Cond 18 AWG Wire	100	ft
9	CAT6 Cable 50' (2 end RJ 45 Terminated)	1	each
10	2 Cond 18 AWG Wire	200	ft

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 399 of 430	

Table B-7. ACS/IDS Bill of Materials – MOW Building

Item	Description	Quantity	Unit
1	ACS/IDS Enclosure	1	each
1.1	Access Control Panel	1	each
1.2	Card reader Controller	2	each
1.3	Input / Output Panels	2	each
1.3	Power Distribution Panels	2	each
1.4	Power Cable 50'	1	each
1.5	Enclosure Wiring kit	1	each
1.6	Enclosure Mounting Bracket	1	each
1.7	Power Cable 50'	1	each
1.8	Terminal Blocks	4	each
1.9	DIN Rail	2	each
2	Request to Exit	15	each
3	Card Reader	15	each
4	Electric Door Strike/lock	15	each
5	Surface Alarm Contact	15	each
6	Motion Sensor	15	each
7	Arming Station	1	each
8	5 Cond 18 AWG Wire	3000	ft
9	CAT6 Cable 50' (2 end RJ 45 Terminated)	1	each
10	2 Cond 18 AWG Wire	1250	ft
11	Terminal Blocks, Screw Connector	15	each
12	2 Cond 18 AWG	100	ft

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 400 of 430	

Table B-8. ACS/IDS Bill of Materials – Wheel Truing Facility

Item	Description	Quantity	Unit
1	ACS/IDS Enclosure	1	each
1.1	Access Control Panel	1	each
1.2	Card reader Controller	2	each
1.3	Input / Output Panels	2	each
1.3	Power Distribution Panels	2	each
1.4	Power Cable 50'	1	each
1.5	Enclosure Wiring kit	1	each
1.6	Enclosure Mounting Bracket	1	each
1.7	Power Cable 50'	1	each
1.8	Terminal Blocks	4	each
1.9	DIN Rail	2	each
2	Request to Exit	2	each
3	Card Reader	2	each
4	Electric Door Strike	2	each
5	Surface Alarm Contact	2	each
6	Motion Sensor	2	each
7	Arming Station	1	each
4	2 Cond 18 AWG Wire	200	ft

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 401 of 430	

Table B-9. ACS/IDS Bill of Materials – Train Wash Facility

Item	Description	Quantity	Unit
1	ACS/IDS Enclosure	1	each
1.1	Access Control Panel	1	each
1.2	Card reader Controller	2	each
1.3	Input / Output Panels	2	each
1.3	Power Distribution Panels	2	each
1.4	Power Cable 50'	1	each
1.5	Enclosure Wiring kit	1	each
1.6	Enclosure Mounting Bracket	1	each
1.7	Power Cable 50'	1	each
1.8	Terminal Blocks	4	each
1.9	DIN Rail	2	each
2	Request to Exit	2	each
3	Card Reader	2	each
4	Electric Door Strike	2	each
5	Surface Alarm Contact	2	each
6	Motion Sensor	2	each
7	Arming Station	1	each
4	2 Cond 18 AWG Wire	200	ft

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 402 of 430	

Appendix C. Spare Parts List

Table C-1 presents a summary of the supplied equipment quantities for the ACS; this information is extracted from the Bill of Materials (BOM); refer to the following reference materials for actual documents.

HNL Directory: HNL-60211 Spare Parts List by System.

Document Title: 3HR-79101-FFBA-XAZZA-01P07-HNL-60211 Spare Parts List.doc.

Table C-1. Spare Part Item Quantities Summary

Subsystem / Description of the LRU	MTBF (Hours)	Failure Rate (failures/hour)	Total Quantities
Intrusion Alarm Control Panel	11,000	9.09E-05	24
IDS Keypad	60,000	1.67E-05	37
Intrusion Detection Horn	180,000	5.56E-06	40
Intrusion Alarm Control Panel	11,000	9.09E-05	24
Ethernet Communication Module	40,000	2.50E-05	45
8-Input Expander Module	40,000	2.50E-05	203
IDS NAC Module	250,000	4.00E-06	34
Intrusion Alarm Control Panel Transformer	311,778	3.21E-06	22
IP Controlled Quad Relay	30,000	3.33E-05	9
Magnetic Contact	48,000	2.08E-05	9
Fence Flexzone Processor Module	257,000	3.89E-06	3
Fence Power Supply	80,000	1.25E-05	2
Fence Ultralink Relay Module	1,158,000	8.64E-07	2
Fence Ultralink Power Supply	80,000	1.25E-05	2
E-Mech Assy, Ultralink I/O Processor Card	250,000	4.00E-06	1
E-Mech Assy, USB To Fiber/422 Converter	105,120	9.51E-06	1
Synergis Master Controller, SMC, W/Onboard Ethernet And	40,000	2.50E-05	27
Mercury Mr16IN 16-Input Monitor Module	160,000	6.25E-06	73
Mercury Mr16OUT 16-Relay Output Monitor Module	160,000	6.25E-06	106
Mercury MR52 2-Reader Interface Module	150,000	6.67E-06	217
12vdc Module Power Supply	60,000	1.67E-05	40
12/24vdc Lock Power Supply	60,000	1.67E-05	33
Door Status Sensor	1,000,000	1.00E-06	304
Micro Switch	1,000,000	1.00E-06	602
Proximity Card Reader	40,000	2.50E-05	262
Request For Exit Interface	80,000	1.25E-05	253
Micro Switch Interface	200,000	5.00E-06	143
Knox Box	170,000	5.88E-06	25

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 403 of 430

Subsystem / Description of the LRU	MTBF (Hours)	Failure Rate (failures/hour)	Total Quantities
Electric Door Lock Interface	70,080	1.43E-05	258
Glass Break Sensor	80,000	1.25E-05	16
Key Switch	100,000	1.00E-05	281
Roll-Up Door Status Sensor	1,000,000	1.00E-06	122
Telephone Entry	40,000	2.50E-05	2
Booth Pushbutton	2,000,000	5.00E-07	3
Gate Interface	96,360	1.04E-05	3
Loop Detector	40,000	2.50E-05	3
Card Reader Pedestal	135,000	7.41E-06	1
12/24VDC Power Supply	60,000	1.67E-05	10
Access Server	180,000	5.56E-06	15
1 Bosch G Series Intrusion Panel Connection	25,000	4.00E-05	12
Domain Controller	180,000	5.56E-06	3
Signature Pad	45,000	2.22E-05	3
Ethernet Converter	90,000	1.11E-05	2
20VA Transformer	61,320	1.63E-05	2
40VA Transformer	61,320	1.63E-05	2
Badge Printer	50,000	2.00E-05	2

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 404 of 430

Appendix D. Product Tree and Asset List

Refer to the following reference file for the CCTV, ACS, and IDS product tree and asset list.

HNL Directory: HNL-66001

Document Title: HNL-66001 06.00-2-Communications System-Appendix 2 - Product Breakdown
Structure_Final.xls

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 405 of 430	

Appendix E. Data Sheets

Table E-1 is a list of data sheets; refer to the following reference materials for actual documents.

HNL Directory: 60122

Document Title: HNL-60122 03.00-0-Communications System-CCTV System Datasheets - Document-Clean.doc

Table E-1. Data Sheets

Number	Name of Data Sheet PDF
1	HNL-60126 06.00-1- 4C001 Genetec Synergis Cloud Link.pdf
2	HNL-60126 06.00-2- 4C002 Genetec Mercury Security MR-16IN.pdf
3	HNL-60126 06.00-3- 4C003 Genetec Mercury Security MR-16OUT.pdf
4	HNL-60126 06.00-4- 4C004 Genetec Mercury Security MR-52.pdf
5	HNL-60126 06.00-5- 4C005 Atlas Sound VTD1-16.pdf
6	HNL-60126 06.00-6- 4C006 Altronix R615DC1016.pdf
7	HNL-60126 06.00-7- 4C007 Altronix MAXIMAL33RD.pdf
8	HNL-60126 06.00-9- 4C010 GE 1076D Recessed Door Contact.pdf
9	HNL-60126 06.00-10- 4C011 Sentrol 1045 Position Sensors.pdf
10	HNL-60126 06.00-11- 4C012 HID 920P multiCLASS SE Readers.pdf
11	HNL-60126 06.00-12- 4C013 Bosch DS150i REX Detector & TP160 Trim Plate.pdf
12	HNL-60126 06.00-13- 4C016 Knox Box 3262.pdf
13	HNL-60126 06.00-14- 4C021 Honeywell FG-730.pdf
14	HNL-60126 06.00-15- 4C022 Camden CM1170-7024 Key Switch.pdf
15	HNL-60126 06.00-16- 4C023 GE 2200A-L Overhead Door Magnetic Contacts.pdf
16	HNL-60126 06.00-17- 4C024 Ameristar Gate 1837AGS Telephone Entry.pdf
17	HNL-60126 06.00-18- 4C034 Sentrol 2105 Heavy-Duty Magnetic Contacts.pdf
18	HNL-60126 06.00-19- 4C035 DynaLOCK 6270 Push Button.PDF
19	HNL-60126 06.00-20- 4C046 BCDVideo BCD360V8.pdf
20	HNL-60126 06.00-21- 4C047 BCDVideo BCD230T.pdf
21	HNL-60126 06.00-22- 4C048 SWHOUSE 20K758USB-SYS.pdf
22	HNL-60126 06.00-23- 4C049 HID HDP5000.pdf
23	HNL-60126 06.00-24- 4C037 Bosch ISC-CDL1 & B328.pdf
24	HNL-60126 06.00-25- 4C056 BCDVideo BCD320E8-M-SAS-MP-C.pdf
25	HNL-60126 06.00-26- 4C057 BCDVideo BCD104-170-MP-C.pdf
26	HNL-60126 06.00-27- 4C038 GE 2507A.pdf
27	HNL-60126 06.00-28- 4C039 GE 2507AD.pdf
28	HNL-60126 06.00-29- 4C040 EPS 3416D.pdf
29	HNL-60126 06.00-30- 4C041 EPS PFL46.pdf
30	HNL-60126 06.00-31- 4C042 PedestalCEO 72-9C-D & LANDO-KY-20x14E.pdf
31	HNL-60126 06.00-32- 4C044 AlarmSaf RM-PS5-MD-UL.pdf
32	HNL-60126 06.00-34- 4C058 Middle Atlantic RM-KB-LCD19.pdf
33	HNL-60126 06.00-35- 4C059 2U Lockable Drawer-162-920.pdf

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 406 of 430

Table E-1. Data Sheets

Number	Name of Data Sheet PDF
34	HNL-60126 06.00-36- 4C050 Genetec GSC-BASE-5.7 Software.pdf
35	HNL-60126 06.00-37- 4C051 Genetec GSC-PM-STD-SITELICENSE Software License.pdf
36	HNL-60126 06.00-38- 4C060 Signature Pad.pdf
37	HNL-60126 06.00-39- 4C061 HID 1386-LGGMN.pdf
38	HNL-60126 06.00-40-4C062-HID Proximity card System1.pdf
39	HNL-60126 06.00-41-4C063 Genetec Declaration of Conformity_DoC.pdf
40	HNL-60126 06.00-41-4C064- Genetec Declaration of Conformity_DoC_Addtional1.pdf
41	HNL-60126 06.00-41-4C065 Mercury Security Declaration of Conformity_DoC.pdf
42	HNL-60126 06.00-41-4C066 HID Global Declaration of Conformity_DoC.pdf
43	HNL-60126 06.00-41-4C067 Altronix Declaration of Conformity_DoC.pdf
44	HNL-60126 06.00-41-4C068 Firewall CABLE-LSZH.pdf
45	HNL-60126 06.00-41-4C069- HP LaserJet Ink Printer 712D.pdf

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 407 of 430

Appendix F. Licenses

Table F-1 is a list of licenses for ACS software and hardware equipment.

Table F-1. List of ACS Licenses

Subsystem / Description of the LRU
GSC- 5.7
GSC- Base 5.7
GSC-Sy-E
GSC-Om-E
GSC-1AD-USCH
GSC-ISTU
GSC-1AP-Bosch
GSC-1SCFED
GSC-1MobileSTU
GSC-1FOD
Sy-MR52
Sy-MR16IN
Sy-MR16OUT
GSC-Threat Levels
GSC-PM-STD SiteLicense
GSC-PM-Advanced
GSC-1SDK-AGENTVI-savVi
GSC-1SDK-OA NetspireIntercom
GSC-Om-E-1C
GSC-Om-E-1FC
Sy-MR52-S3
GSC-Ap-Base

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 408 of 430

Appendix G. Warranties and Technical Support

Table G-1 is a list of warranties and technical support available for ACS software and hardware equipment; refer to the following reference materials for actual documents.

HNL Directory: HNL-61650

Document Title: HNL-61650 02.00-0-Communications Systems - Supplier Maintenance Warranty Information.doc.

OIC Label	Asset Description	Qty	Asset	Manufacturer	Model	Nokia P/N	Segment	LRU	Domain	EOL	EOS	Replacement	Rep EOL	Rep EOS	Comment
4C044-002	12/24V POWER SUPPLY ALARMSAF	10	Equipment	ALARMSAF	PS5-M	1AF30614AAAA	1	Yes	ACS						
4C006-004	12VDC MODULE POWER SUPPLY	47	Equipment	Altronix	R615DC1016	1AK08863AKAA	1	Yes	ACS	No Plan	No Plan	NA	NA	NA	
4C007-002	12/24VDC LOCK POWER SUPPLY	33	Equipment	Altronix	MAXIMAL33RD	1AK07668AAGA	1	Yes	ACS	No Plan	No Plan	NA	NA	NA	
4C009-001	ACCESS CONTROL UPS BATTERY PACK	2	Equipment	APC	SMC1000-2U	N/A	1	Yes	ACS						
4C045-001	SMALL ACS UNINTERRUPTIBLE POWER SUPPLY	1	Equipment	APC	SMX2000RMLV2U	N/A	1	Yes	ACS						
4C045-003	ACCESS CONTROL UPS BATTERY PACK	16	Equipment	APC	SMC1000-2U	N/A	1	Yes	ACS						
4*W0*014/1-001	BCDVIDEO WORKSTATION COMPUTER	4	Component	BCDvideo	BCD230T-M-141416	N/A	1	Yes	ACS	N/A					BCDvideo
4C046-001	DIRECTORY SERVER	15	Equipment	BCDvideo	BCD360V8-M-MP-C	N/A	1	Yes	ACS			SERVER360 SER150			
4C057-002	Domain Controller -APP	3	Equipment	BCDvideo	BCD104V-120-MP-C-KIT	1Ak08979AAAA	1	Yes	ACS			Controller360 troller30			
4C037-002	MOTION DETECTOR	1	Equipment	Bosch	DS970	N/A	1	Yes	ACS	TBD	TBD	NA	NA	TBD	No EOL issue
4C022-001	Key Switch	330	Equipment	Camden	CM-1170-7024	1AK07668AALA	1	Yes	ACS	TBD	TBD	NA	NA	NA	no EOL issue
4B012-001	QUAD IP CONTROLLED RELAY	9	Equipment	CBW	X-WR-4R3-E	1AK16403AAAA	1	Yes	ACS						
4C024-004	TELEPHONE ENTRY	3	Equipment	Doorking	1837-080 Surface	1AK14804AAAA	1	Yes	ACS						
4C062-002	TCP/IP to RS232 Ethernet Converter Server Kit 10M/100M part of 4C024	3	Equipment	Doorking	USR-TCP232-410-DK	N/A	1	Yes	ACS						
4C035-003	BOOTH PUSHBUTTON MOM SPDT 2 in SQ	3	Equipment	DynaLOCK	N/A	1AK07668AANA	1	Yes	ACS						
4*W0*031/1-001	DB9 Serial Y-Cable 2 Male to 1 Female	6	Cable	E-Filliate Inc.	N/A	N/A	1	Yes	ACS						

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System Operations Manual		Page 409 of 430

OIC Label	Asset Description	Qty	Asset	Manufacturer	Model	Nokia P/N	Segment	LRU	Domain	EOL	EOS	Replacement	Rep EOL	Rep EOS	Comment
4C040-001	LOOP DETECTOR	3	Equipment	EPS	3416D	1AK07668AARA	1	Yes	ACS						
4C041-003	LOOP DETECTOR CABLE	3	Equipment	EPS	PR46	N/A	1	Yes	ACS						
4C049-001	BADGE PRINTER HDP5000	2	Equipment	Fargo	6700019NI	N/A	1	Yes	ACS						
4C010-001	DOOR STATUS SENSOR	356	Equipment	GE/Sentrol	N/A	1AK07668AAHA	1	Yes	ACS						these are magnets. No EOL issue
4C011-003	MICRO SWITCH	640	Equipment	GE/Sentrol	N/A	1AK08863AAAA	1	Yes	ACS						these are magnets. No EOL issue
4C034-003	LOUVER TAMPER SWITCH	17	Equipment	GE/Sentrol	N/A	1AK08131AAAA	1	Yes	ACS						these are magnets. No EOL issue
4C038-002	ATC 1 POTENTIAL-FREE CONTACT	10	Equipment	GE/Sentrol	N/A	N/A	1	Yes	ACS						these are magnets. No EOL issue
4C039-001	ATC 2 POTENTIAL-FREE CONTACT	45	Equipment	GE/Sentrol	2507-AD	1AK07668AAQA	1	Yes	ACS						these are magnets. No EOL issue
4C001-001	SYNERGIS MASTER CONTROLLER Cloudlink	27	Equipment	Genetec	SY-CLOUDLINK	1AK07668AACA	1	Yes	ACS						
4C002-001	MERCURY MR16IN 16-INPUT MONITOR MODULE	77	Equipment	Genetec	SY-MR16IN	1AK08863APAA	1	Yes	ACS						
4C003-001	MERCURY MR16OUT 16-RELAY OUTPUT MONITOR MODULE	122	Equipment	Genetec	SY-MR16OUT	1Ak07668AADA	1	Yes	ACS						
4C004-001	MERCURY MR52 2-READER INTERFACE MODULE	224	Equipment	Genetec	SY-MR52	1AK07668AAEA	1	Yes	ACS						
4C026-001	Rack Mount Shelf with SMC Cloudlink	47	Equipment	Genetec	SMC Shelf	1AK09770AAAA	1	Yes	ACS						

Document	HNL-62708	Revision	XX.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-60XXX XX 00-o-COMMS SYSTEM – Security System: Genetec Synergis, Access Control System (ACS) Operations Manual		Page 410 of 430

OIC Label	Asset Description	Qty	Asset	Manufacturer	Model	Nokia P/N	Segment	LRU	Domain	EOL	EOS	Replacement	Rep EOL	Rep EOS	Comment
4C028-001	ACS 2x MR52 Module Shelf	112	Equipment	Genetec	2MR52 Shelf	1AK09771AAAA	1	Yes	ACS						
4C029-002	ACS 1x MR16IN Module Shelf	39	Equipment	Genetec	1MR16N Shelf	1AK09773AAAA	1	Yes	ACS						
4C031-002	ACS 1x MR16OUT Module Shelf	23	Equipment	Genetec	1MR16O Shelf	N/A	1	Yes	ACS						
4C050-001	Genetec Security Center (GSC) Base Package	1	Software	Genetec	GSC-Base 5.3	N/A	1	Yes	ACS						
4C051-001	Plan Manger for unlimited entities	1	Software	Genetec	GSC-PM-STD-Site license	N/A	1	Yes	ACS						
4C052-001	1 Failover Directory Role	1	Software	Genetec	GSC-1FOD	N/A	1	Yes	ACS						
4C053-001	1 Bosch G Series Intrusion Panel	1	Software	Genetec	GSC-1ap-Bosch	N/A	1	Yes	ACS						
4C054-001	GSC Synergis Professional	1	Software	Genetec	GSC-SY-P	N/A	1	Yes	ACS						
4C055-001	SMA for 1 Synergis Pro Reader	1	Software	Genetec	SMA-RDR-P-1Y	N/A	1	Yes	ACS						
4C012-001	PROXIMITY CARD READER	297	Equipment	HID	920PTNNEK00000	1AK07668AAJA	1	Yes	ACS						
4C021-004	GLASS BREAK SENSOR	16	Equipment	Honeywell	FG-730	N/A	1	Yes	ACS						
4C0460001/1-001	HP 450GB 10K SAS HDD	30	Component	HPE	EG0450FCVBH	N/A	1	Yes	ACS	EOL	TBD	872479-B21 - HPE 1.2TB SAS 12G Enterprise 10K SFF	6/1/22	12/31/22	
4C0460002/1-001	HP 900GB 10K SAS HDD	17	Component	HPE	EG0900FCSPN	N/A	1	Yes	ACS	EOL	TBD	872479-B21 - HPE 1.2TB SAS 12G Enterprise 10K SFF	6/1/22	12/31/22	
4C0460003/1-001	HP 900GB 10K SAS HDD	7	Component	HPE	EG0900FBVFQ	N/A	1	Yes	ACS	EOL	TBD	872479-B21 - HPE 1.2TB SAS 12G Enterprise 10K SFF	6/1/22	12/31/22	
4C0460004/1-001	HP 460W FS Plat Ht Plg Pwr Supply Kit	18	Component	HPE	HPE 460W CS Plat PL Ht Plg Pwr Spply Kit	1AK00060AAAA	1	Yes	ACS	EOL	7/18/19	NA	4/5/18	7/31/18	There's no replacement option for the power supply.

Document	HNL-62708	Revision	XX.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-60XXX XX 00-o-COMMS SYSTEM – Security System: Genetec Synergis, Access Control System (ACS) Operations Manual		Page 411 of 430

OIC Label	Asset Description	Qty	Asset	Manufacturer	Model	Nokia P/N	Segment	LRU	Domain	EOL	EOS	Replacement	Rep EOL	Rep EOS	Comment
4C0560001/1-001	2TB 7200rpm SAS HDD	3	Component	HPE	MB2000FCWDF	N/A	1	Yes	ACS	EOL	TBD	872487-B21 - HPE 4TB SAS 12G Midline 7.2K LFF	10/1/21	4/30/22	
4C0570002/1-001	HP 800W/900W Power Supply	6	Component	HPE	HP 800W/900W Gold AC Power Input Modu	N/A	1	Yes	ACS	EOL	1/18/19	W360 Power60	12/1/17	1/31/18	There's no replacement option for the power supply.
4C0570001/1-001	SSD DC S3500 Series 120GB	6	Component	Intel	S3500	N/A	1	Yes	ACS						
4B013-001	Magnetic Contact	8	Equipment	Interlogix	1035	N/A	1	Yes	ACS						
4C016-001	KNOX BOX	25	Equipment	Knox	3200 Series	1AK08863AHAA	1	Yes	ACS	NA	NA				no EOL issue
4B019-001	Fence UltraLink Power Supply, 48V / 0.83A	2	Equipment	MEAN WELL	MDR-40-48	N/A	1	Yes	ACS						
4CW01-001	ACS/IDS Administration Workstation	3	Equipment	N/A	N/A	N/A	1	N/A	ACS						Bundled items: NA for warranty
4CW02-001	ACS/IDS Administration Workstation (Badge Printer)	1	Equipment	N/A	N/A	N/A	1	N/A	ACS						Bundled items: NA for warranty
4C042-001	HOUSING, LANDSCAPE, 20X14X6, BLK for PEDESTAL	1	Equipment	PEDESTALCEO	LANDO-KY-20x14E	N/A	1	Yes	ACS						
4****4S/1-001	Operating System - Red Hat Enterprise Linux Server - Standard V3.4	12	Software	Red Hat	RH00004	N/A	1	Yes	ACS	No Plan	No Plan	NA			licenses are renewed till 11/30/21
4013HNC-085	20 COND 16/18 AWG Shielded and Unshielded Type Q (1,376 ft.)	110	Cable	RSCC	N/A	1AC059310001	1	No	ACS						
4024HNC-018	2/C 18 AWG Stranded XL-LSZH Firewall M4 (10097 ft.)	86	Cable	RSCC	N/A	1AC058470001	1	No	ACS						
4028HNC-001	6/C 18 AWG Stranded Shielded XL-LSZH Type R (4589 ft.)	4	Cable	RSCC	N/A	1AC058470002	1	No	ACS						

Document	HNL-62708	Revision	XX.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-60XXX XX 00-o-COMMS SYSTEM – Security System: Genetec Synergis, Access Control System (ACS) Operations Manual		Page 412 of 430

OIC Label	Asset Description	Qty	Asset	Manufacturer	Model	Nokia P/N	Segment	LRU	Domain	EOL	EOS	Replacement	Rep EOL	Rep EOS	Comment
4029HNC-001	4/C 18 AWG Stranded XL-LSZH Firewall LSZ (1521 ft.) (ACS/IDS)	8	Cable	RSCC	N/A	1AC058440001	1	No	ACS						
4045HNC-002	SENSTAR SIGNAL CABLE (Q1) 500FT	13	Cable	Senstar	N/A	1AC058440001	1	Yes	ACS						
4B014-001	E-MECH ASSY, Flexzone 4 w/Processor Module	4	Equipment	Senstar	N/A	N/A	1	Yes	ACS						
4B014001/1-001	PCB ASSY, SILVER COMM CARD G2 RS422	2	Component	Senstar	N/A	N/A	1	Yes	ACS						
4B015-001	Fence Splice Unit	13	Equipment	Senstar	G6KT0101	N/A	1	No	ACS						
4B016-001	Fence Termination Unit	4	Equipment	Senstar	G6KT0201	N/A	1	Yes	ACS						
4B017-001	Fence Power Supply, 48VDC, 50W	2	Equipment	Senstar	DPP50-48	N/A	1	Yes	ACS						
4B018-001	Fence UltraLink I/O 32 Relay Module	1	Equipment	Senstar	N/A	N/A	1	Yes	ACS						
4B020-001	E-MECH ASSY, UltraLink I/O Processor Card	2	Equipment	Senstar	N/A	N/A	1	Yes	ACS						
4B021-001	E-MECH ASSY, USB to Fiber/422 Converter	1	Equipment	Senstar	N/A	N/A	1	Yes	ACS						
4B022-001	Comm card, multi-mode Fiber optic (MMFO), G2 Silver	2	Equipment	Senstar	N/A	N/A	1	Yes	ACS						
4C048-002	CAMERA Badging	2	Equipment	SWHouse	20K758USB-SYS	N/A	1	Yes	ACS						
4C060-001	Signature Keypad	3	Equipment	Topaz	T-S461-HSB-R	N/A	1	Yes	ACS						
4C063-001	Plug in Class 2 Transformer 20VA part of 4C024	3	Equipment	Universal Power Group	AD48-0001	N/A	1	Yes	ACS						
4C064-001	Plug in Class 2 Transformer 40VA part of 4C024 Doorking	3	Equipment	Universal Power Group	UB1640WR	N/A	1	Yes	ACS						
4C023-001	ROLL-UP DOOR STATUS SENSOR	188	Equipment	UTC	2202A-L-SS	1AK08863ABAA	1	Yes	ACS						

Document	HNL-62708	Revision	XX.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-60XXX XX 00-o-COMMS SYSTEM – Security System: Genetec Synergis, Access Control System (ACS) Operations Manual		Page 413 of 430

Appendix H. OEM User Manuals

Table H-1 is a list of ACS OEM user manuals.

Table H-1. List of OEM User Manuals

#	OEM User Manual
1	Genetec Security Center Installation and Upgrade Guide 5.7 SR
2	Genetec Security Center Administrator Guide 5.7
3	Genetec Security Center 5.7 System Requirements
4	Genetec Security Center 5.7 Ordering Guide
5	Genetec Security Desk User Guide 5.7
6	Getting Started with Security Desk 5.7
7	Security Center 5.7 Network Diagram - Access Control
8	Security Center Best Practices 5.7 Access Control
9	Genetec AC Train Mats-Part 3 Chap 14-19 Synergis Security Desk User Guide 5.2

Document	HNL-62708	Revision	XX.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-60XXX XX 00-o-COMMS SYSTEM – Security System: Genetec Synergis, Access Control System (ACS) Operations Manual	Page 414 of 430	

Appendix I. Typical Layouts and Installation Drawings

Table I-1 is a list of typical layouts and installation drawings for the ICCS; refer to the following reference materials for actual documents.

HNL Directory: HNL-60037

Document Title: HNL-60037-00.00-0-CCTV-Typical Layouts & Install Dwg

Table I-1. List of Typical Layouts and Installation Drawings for ACS

#	Document Name/Description
1	HNL 60037-018 - ACS-IDS STATION OSB LAYOUT AND INSTALLATION.dwg
2	HNL 60037-019 - ACS-IDS OCC LAYOUT AND INSTALLATION.dwg
3	HNL 60037-020 - ACS-IDS B-OCC LAYOUT AND INSTALLATION.dwg
4	HNL 60037-021 - ACS-IDS STATION TCCR LAYOUT AND INSTALLATION.dwg
5	HNL 60037-022 - ACS-IDS STATION MOW LAYOUT AND INSTALLATION.dwg
6	HNL 60037-023 - ACS-IDS STATION WTF LAYOUT AND INSTALLATION.dwg
7	HNL 60037-024 - ACS-IDS STATION TWF LAYOUT AND INSTALLATION.dwg
8	HNL 60037-025 - ACS-IDS STATION YCB LAYOUT AND INSTALLATION.dwg
9	HNL 60037-026 - TYPICAL CAMERA LAYOUT.dwg
10	HNL 60037-027 - TYPICAL CARD READER LAYOUT.dwg

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 415 of 430

Appendix J. System Block Diagrams

Table J-1 is a list of system block diagrams for the ICCS; refer to the following reference materials for actual documents.

HNL Directory: HNL 60036

Document Title: HNL 60036-00.00-CCTV-AC-ID System Block Diagrams.docx

Table J-1. List of System Bloc Diagrams for ACS

#	Document Name/Description
1	HNL 60036-003 - ACS-IDS SYS BLOCK DIAGRAM.dwg
2	HNL 60036-005 - ACS-IDS SYS OSB FACILITY SYS BLOCK DIAGRAM.dwg
3	HNL 60036-007 - ACS-IDS SYS OCC FACILITY SYS BLOCK DIAGRAM.dwg
4	HNL 60036-009 - ACS-IDS SYS BOCC FACILITY SYS BLOCK DIAGRAM.dwg
5	HNL 60036-011 - ACS-IDS SYS MOW FACILITY SYS BLOCK DIAGRAM.dwg
6	HNL 60036-013 - ACS-IDS SYS YCB FACILITY SYS BLOCK DIAGRAM.dwg
7	HNL 60036-015 - ACS-IDS SYS WHEEL TRUING FACILITY SYS BLOCK DIAGRAM.dwg
8	HNL 60036-017 - ACS-IDS SYS TRAIN WASH FACILITY SYS BLOCK DIAGRAM.dwg
9	HNL 60036-019 - ACS-IDS SYS TYPICAL STATION FACILITY SYS BLOCK DIAGRAM.dwg

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 416 of 430

Appendix K. Software Requirements

Tables K-1 and K-2 provide a list of the software requirements for ACS.

K1. SOFTWARE REQUIREMENTS

Table K-1. ACS Software Requirements - Version

Application	Version
Genetec Security Center	5.7 SR3
Genetec Security Desk	5.7 SR3

Table K-2. ACS Software Requirements

System	Options
Operating System	- Microsoft® Windows 10 Pro/Enterprise¹ - Microsoft® Windows 8.0/8.1 Pro/Enterprise1 - Microsoft® Windows 7 Pro/Enterprise/Ultimate SP1¹ - Microsoft® Windows Server 2008 SP2^{1,2} - Microsoft® Windows Server 2008 R2² - Microsoft® Windows Server 2012/2012 R2²
Browsers for Server Admin	- Internet Explorer 9, 10, and 11 - All web browsers that support HTML 5
Browsers for SCL Portal	Internet Explorer 9, 10, or Google Chrome
Database Engines	- SQL Server 2008 R2 Express/Standard/Enterprise - SQL Server 2012 Express/Standard/Enterprise - SQL Server 2014 Express/Standard/Enterprise
Virtualization (Server)	- VMware ESXi 5.x - VMware ESXi 6.x - Microsoft® Hyper-V with Windows Server 2012 or Windows Server 2012 R2
Clustering (Server)	- Microsoft® Windows Server 2008/2008 R2/2012/2012 R2 - NEC ExpressCluster X R3 WAN/LAN Editions for Windows v.3.0.0.1

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 417 of 430

K2. WORKSTATION HARDWARE REQUIREMENTS

Table K-3 provides a list of the workstation hardware requirements for ACS.

Table K-3. ACS Workstation Requirements

System	Requirements
Minimum	- Intel Core 2 X6800 @ 2.93 GHz 2 GB of RAM 80 GB hard drive for OS and <i>Security Center</i> applications 256 MB PCI-Express x16 dual-head video adapter 1280 x 1024 or higher screen resolution 100/1000 Ethernet Network Interface Card 16x DVD+/- RW Drive
Recommended	4th Generation Intel® Core™ i7-4770 or better 8 GB of RAM or better 64-bit operating system 120 GB Solid State Drive for OS and <i>Security Center</i> applications - GbE network interface card - NVIDIA® QUADRO K620 2 GB video card
High Performance (Video intensive configuration)	4th Generation Intel® Core™ i7-4770 or better 16 GB of RAM or better 64-bit operating system 240 GB Solid State Drive for OS and <i>Security Center</i> applications - GbE network interface card 2 x NVIDIA® GeForce® GTX 970 4 GB video card
General Notes	- Minimum of 2 GB of video RAM recommended - NVIDIA® Maxwell-based GPU recommended - Intel® Quick Sync Video is recommended only if the Intel discrete graphics card is directly connected to a display device - Two or more graphic cards can be used to support different monitors individually. To have the video decoding done on the card, at least one monitor must be connected to each card - NVIDIA® SLI™ bridge not supported - For a list of compatible video cards with hardware acceleration, contact the Genetec Sales Engineering Team
Notes: ¹ Config Tool requires a minimum resolution of 1024 x 768. Not required for virtual servers. ² The intended throughput requires specific hardware and software configurations.	

K3. MAXIMUM NUMBER OF CAMERAS VIEWED PER CLIENT TYPE

To ensure that your client workstation runs optimally, it is important to know the maximum number of cameras that can be viewed per client station type in *Security Center* 5.7. The maximum number of cameras viewed per client station type in *Security Center* 5.7 is as follows.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 418 of 430

Table K-4. Maximum Number of Cameras Viewed Per Client Type

H.264 format	CIF	VGA	HD	Full HD	Ultra HD
Resolution @ 30 fps	352 x 240	640 x 480	1280 x 720	1920 x 1080	3840 x 2160
Average bit rate/camera ¹	350 Kbps	1 100 Kbps	2 300 Kbps	5 500 Kbps	50 000 Kbps
Minimum	14	6	2	1	0
Recommended ²	60	47	23	11	6
High performance ^{2, 3} Video intensive configuration	78	58	50	26	8
Notes ¹ These are estimates, and different camera manufacturer's bit rate may vary with the same resolution and frame rate. The decoding performance can also vary from one manufacturer to another. ² With hardware acceleration enabled. ³ Using one video card NVIDIA® GeForce GTX 1060 with 6 GB of RAM.					

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 419 of 430	

K.4 PERFORMANCE BENCHMARK FOR HEVC (H.265)

The following benchmark illustrates the average bit rate of a camera streaming at 20 fps using HEVC (H.265) video format. The viewing workstation has a 4th Generation Intel Core™ i7-4770 @ 3.5 GHz processor, with 16 GB RAM, an SSD hard drive, and runs Windows 8.1. The video card used is an NVIDIA GeForce® GTX 1060, with 6 GB of RAM connected to a 4K monitor.

Table K-5. Performance Benchmark for HEVC (H.265)

H.265 format	VGA	HD	UXGA	Full HD
Resolution @ 20 fps	640 x 480	1280 x 720	1600 x 1200	1920 x 1080
Average bit rate/camera ¹	150 Kbps	445 Kbps	730 Kbps	50 000 Kbps
Maximum Number of Cameras	77	51	31	24

K.5 MAXIMUM NUMBER OF CAMERAS AND READERS PER SERVER TYPE

To ensure that your system runs optimally, it's important to know the maximum number of cameras and readers per server type in *Security Center 5.7*.

Table K-6. Maximum Number of Cameras Viewed per Client Type

Server Type	Minimum	Recommended
Directory & Archiver (Video only)	50 cameras or 50 Mbps	100 cameras or 200 Mbps
Standalone Archiver (Video only)	75 cameras or 75 Mbps	300 cameras or 300 Mbps ¹
Directory & Access Manager (Access control only)	100 HID Edge readers/ V2000, or 150 readers on HID V1000/Synergis™ Cloud Link 10 HID V1000/Synergis™ Cloud Link 10,000 cardholders	300 HID Edge readers/V2000, or 300 readers on HID V1000 or 1024 readers on Synergis™ Cloud Link 100 HID V1000/Synergis™ Cloud Link 250,000 cardholders
Standalone Access Manager (Access control only)	100 HID Edge readers/ V2000, or 150 readers on HID V1000/Synergis™ Cloud Link 10 HID V1000/Synergis™ Cloud Link 10,000 cardholders	700 HID Edge readers/V2000, or 500 readers on HID V1000 or 2048 readers on Synergis™ Cloud Link 100 HID V1000/Synergis™ Cloud Link 250,000 cardholders
Directory, Archiver & Access Manager (Unified)	50 cameras or 50 Mbps and 64 readers 5 HID V1000/Synergis™ Cloud Link 5,000 cardholders	100 cameras or 200 Mbps and 200 readers 40 HID V1000/Synergis™ Cloud Link 40,000 cardholders
Note: ¹ For high-performance Archivers (500 cameras and up), see <i>Security Center 5.7</i> server requirements		

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 420 of 430

Appendix L. Software Release Notes & Lifecycle Data

L.1 PRODUCT LIFECYCLE

Modern software evolves at a rapid pace. Genetec constantly updates its products to keep up with customer needs as they develop. Maintaining the growing number of product versions introduces new challenges. We are addressing these challenges and reducing risks associated with outdated software by establishing a clear product lifecycle policy. Defining a lifecycle policy for our software is an important step in continuing to deliver consistent service for customers.

Genetec is proud to deliver industry-leading products and support programs that allow you to tap into the full potential of your security system. Towards this end, Genetec provides continuous support throughout the lifetime of its products. Customers can benefit from a variety of services, including technical assistance, product training and certification, software updates, security fixes, emergency hotfixes, product documentation, and more.

The Genetec product lifecycle policy provides a clear overview of product availability, support, and services available throughout all the stages of a product's lifecycle, from General Availability to End of Life (EOL).

L.2 SECURITY CENTER LIFECYCLE RELEASE TRACKS

To provide access to new functionalities and support the latest devices, *Security Center* uses a continuous delivery model for its core systems and add-on modules. This model consists of two software release track: the Continuous Delivery (CD) track and the Long-Term Support (LTS) track:

- Releases on the CD track include access to new features, performance enhancements, supported devices, and integration capabilities in addition to the latest security and defect fixes. Releases on the CD tracks are supported for 3 years.
- For clients who want to limit the frequency of functional updates, releases on the LTS track include a subset of security and defect fixes that have limited or no impact on system architecture. Releases on the LTS track are supported for 5 years.

L.3 RELEASE TYPES

Security Center versions contains four digits:

5.8.1.3

(A) (M) (mi) (p)

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 421 of 430	

Table L-1. Security Center Release Types

Digit	Release Type	Description
(A)	Architecture	- Release that introduces significant changes to the architecture or user experience of the platform. Architecture upgrades require changes to system design, hardware, reconfiguration of settings, and re-training of users. - Architecture versions are not backward-compatible with previous versions. - A license update is required to upgrade to a new Architecture release. - Available on the CD and LTS tracks.
(M)	Major	- Release that contains new features, behavioral changes, SDK capabilities, support for new devices, and performance improvements. Major versions are backward-compatible with clients and servers using one of the three previous Major versions (e.g., 5.8.x.x is compatible with all 5.7, 5.6, and 5.5 releases) using Backward compatibility mode¹. - A license update is required to upgrade to a new Major release. - Available on the CD and LTS tracks.
(mi)	Minor	- Release that contains new features, SDK capabilities, support for new devices, bug fixes, and security fixes. - Minor releases are backward-compatible with clients and servers running one of the three previous Major versions (e.g., 5.8.1.x is compatible with all 5.7, 5.6, and 5.5 releases) using Backward compatibility mode¹. - No license update is required to upgrade to a new Minor release. - Available only on the CD track.
(p)	Patch	- Release that contains support for new devices, bug fixes, and security fixes. - Patch releases are backward-compatible with clients and servers running one of the three previous Major versions (e.g., 5.8.1.1 is compatible with all 5.7, 5.6, and 5.5 releases) using Backward compatibility mode¹. - No license update is required to upgrade to a new Patch release. - Available on the CD and LTS tracks. Please note that LTS patch releases are limited to certain bug and security fixes.
Notes: ¹ Backward compatibility mode impacts performance and features. Please consult the <i>Security Center</i> installation and upgrade guide for limitations. ² New Minor versions are only available during the GA stage of a Major version's lifecycle. Once a new Major version is available; only new Patches will be released until the version's End of Sale.		

L.4 LIFECYCLE STAGES

Major versions of the *Security Center* go through four lifecycle stages. Each stage determines the types of new releases issued, the types of fixes available without upgrading to a recent Major version, and the commercial availability of licenses.

General Availability: Begins when a Major version is available for purchase.

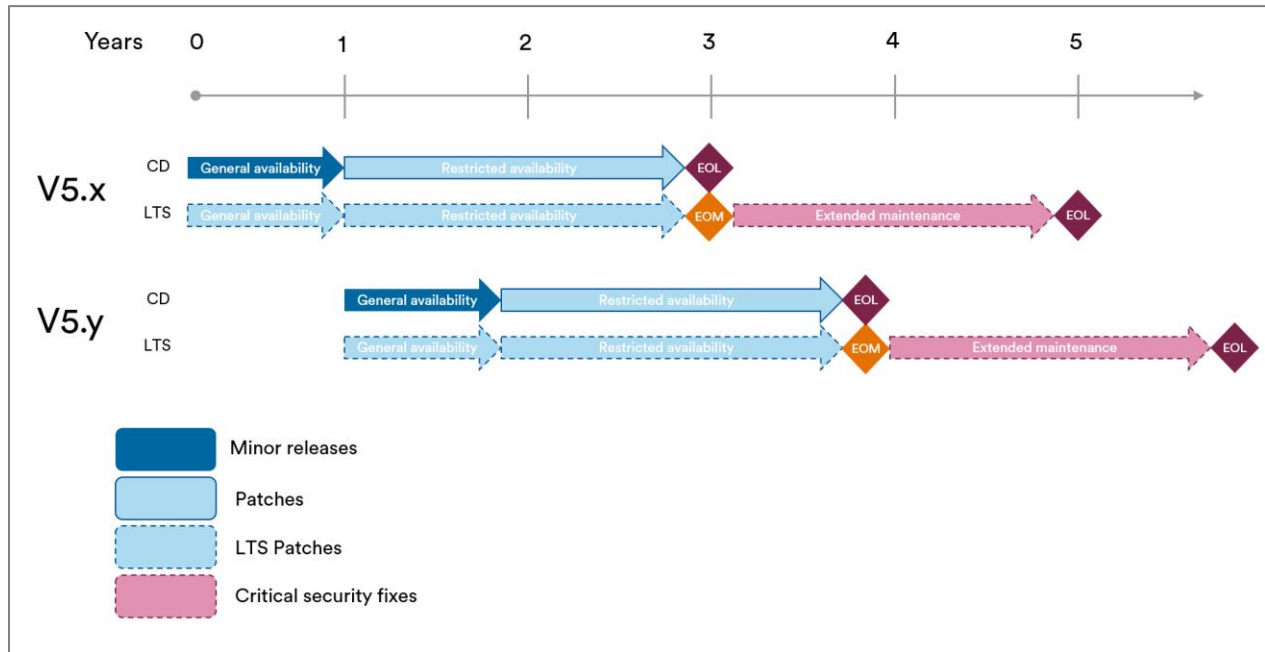
Restricted Availability: Begins when a subsequent Major version is available for purchase.

End of Maintenance: Occurs 3 years after the General Availability of a Major version.

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 422 of 430

End of Life: Occurs 5 years after the General Availability of a Major version.

The diagram below highlights the standard lifecycle stages and release types throughout a major version's lifecycle.



Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 423 of 430	

L.5 PRODUCT LIFECYCLE POLICY SUMMARY

Genetec reserves the right to extend each stage of a major version's lifecycle. Table L-2 details the services and updates available for each stage.

Table L-2. Product Lifecycle Stages

Product Release & Support	General Availability	Restricted Availability	End of Maintenance	End Of Life (EOL)
Product available for sale (new systems and new end users)				
Product available for an extension to an existing system				
Technical support available	1	1	1	
Genetec product certification available				
New Minor releases				
New Patch releases				
Hotfixes for critical bugs and security issues	2	2	2	
Documentation available on website				
License maintenance				
Notes: ¹ Online general assistance with Genetec™ Assurance; optional advanced troubleshooting and live support through Genetec™ Advantage. ² Requires Genetec™ Advantage.				

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 424 of 430	

L.6 PRODUCT LIFECYCLE TIMELINE

Table L3. Synergis Softwire Product Lifecycle Policy Summary

	General Availability	Restricted Availability
Product available for sale (new systems and new end users)		
Product available for an extension to the existing system		
Technical support available		
Security fixes		
Emergency hotfixes availability		
Documentation available on website		
Note: 1 EOL is around 2 years after the next version is released.		

Table L4. Synergis Softwire Product Lifecycle Timeline

Product	Current Stage in Lifecycle	General Availability	Restricted Availability
Synergis Softwire 10.11	General availability	7-Jan-2020	TBA*
Synergis Softwire 10.10	Restricted availability	23-Jul-2019	1-Mar-2020
Synergis Softwire 10.9	General availability	07-Feb-2019	1-Mar-2020
Synergis Softwire 10.8	Restricted availability	07-Aug-2018	30-May-2019
Synergis Softwire 10.7	Restricted availability	17-Apr-2018	07-Aug-2018
Synergis Softwire 10.6	Restricted availability	15-Jan-2018	17-Apr-2018
Synergis Softwire 10.5	Restricted availability	19-Jul-2017	15-Jan-2018
Synergis Softwire 10.4	Restricted availability	16-Jan-2017	19-Jul-2017
Synergis Softwire 10.3	Restricted availability	25-Jul-2016	16-Jan-2017
Synergis Softwire 10.2	Restricted availability	19-Apr-2016	25-Jul-2016
Synergis Softwire 10.1	Restricted availability	12-Dec-2015	19-Apr-2016
Synergis Softwire 10.0	Restricted availability	25-Jun-2015	12-Dec-2015
Legal Disclaimer The information contained herein is used as a reference point for the Genetec product lifecycle policy. It is not a legally binding document and does not confer legal obligations for Genetec. Some products are subject to exceptions and are flagged in the tables above. Genetec may decide to extend the lifecycle of certain products or modify this policy at any time, which will be communicated in an appropriate manner. Genetec, Omnicast, and the Genetec logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.			

Table L-5. Product Lifecycle Timeline

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 425 of 430

Table L4. Synergis Software Product Lifecycle Timeline

Product		Current Stage in Lifecycle		General Availability	Restricted Availability	
Product	Current Stage in Lifecycle	General Availability	Restricted Availability	End of Maintenance	End of Sale (EOS)	End of Life (EOL)
Security Center 5.8	General availability	10-May-2019	TBA*	TBA*	TBA*	TBA*
Security Center 5.7	Restricted availability	14-Jun-2019	10-May-2019	31-May-2020	TBA*	31-May-2023
Security Center 5.6	General availability	10-Apr-2017	21-Nov-2017	30-Nov-2018	30-Nov-2020	30-Nov-2021
Security Center 5.5	Restricted availability	20-Jul-2016	10-Apr-2017	31-Mar-2018	31-Mar-2020	31-Mar-2021
Security Center 5.4	Restricted availability	4-Jan-2016	20-Jul-2016	20-Jul-2017	30-Jun-2019	30-Jun-2020
Security Center 5.3	Restricted availability	19-May-2015	4-Jan-2016	4-Jan-2017	31-Dec-2018	31-Dec-2019
Security Center 5.2	End of Sale (EOS)	5-Apr-2013	19-May-2015	19-May-2016	30-Jun-2018	30-Jun-2019
Security Center 5.1	End of Life (EOL)	16-Jan-2012	--	--	31-Dec-2017	30-Jun-2018
Security Center 5.0	End of Life (EOL)	20-Apr-2011	--	--	31-Dec-2017	30-Jun-2018
Security Center 4.0	End of Life (EOL)	22-Apr-2010	--	--	30-Jun-2017	31-Dec-2017
Security Center 3.0	End of Life (EOL)	16-Sep-2009	--	--	28-Feb-2013	31-Dec-2013
Note: ¹ Dependent on the next software release.						

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 426 of 430

L.7 SECURITY CENTER ADD-ON**Table L-6. Security Center Add-On Product Lifecycle Policy Summary**

Support	General Availability	End of Sale (EOS)	End of Life (EOL)
Product available for sale (new systems and new end users)			
Product available for an extension to the existing system			
Technical support available	1	Requires Genetec Advantage	
Emergency hot fixes availability	1	Requires Genetec Advantage	
Documentation available on website			
License maintenance			
Notes: ¹ Online general assistance with Genetec™ Assurance; optional advanced troubleshooting and live support through Genetec™ Advantage Product Lifecycle Timeline.			

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 427 of 430	

Table L-7. Plugin Product Lifecycle

Plugin	Status	General Availability	End of Sale (EOS)	End Of Life (EOL)
Barco CMS	General availability	6-Nov-2015	31-Mar-2020	TBA*
Bosch B or G series	General availability	20-Mar-2013	31-Mar-2020	TBA*
Bosch Intrusion Panel Extension 4.0	General availability	23-Nov-2016	30-Nov-2020	TBA*
CCURE Access Control	General availability	2-Feb-2015	30-Nov-2020	TBA*
CCURE Video Integration	General availability	2-Feb-2015	30-Nov-2020	TBA*
DSC Power Series 4.0	End of Sale (EOS)	27-Aug-2013	–	30-Jun-2020
ID Scanner 3.0	General availability	–	30-Nov-2020	TBA*
Lenel OnGuard	End of Life (EOL)	13-Mar-2014	–	1-Dec-2019
Lenel Video Translator	End of Life (EOL)	13-Mar-2014	–	1-Dec-2019
OPC Client 3.0	General availability	26-Jun-2017	30-Nov-2020	TBA*
Panasonic_DVR	End of Life (EOL)	15-Jan-2015	–	1-Dec-2019
RFCode 3.1	End of Life (EOL)	12-Mar-2013	–	1-Dec-2019
Southwest Microwave INTREPID MicroPoint I 3.0	End of Life (EOL)	14-Mar-2013	–	1-Dec-2019
Southwest Microwave INTREPID MicroPoint II 3.0	End of Life (EOL)	16-Mar-2018	–	1-Dec-2019
ThyssenKrupp 3.0	End of Life (EOL)	12-Mar-2013	–	1-Dec-2019
Vanderbilt SPC extension 3.0	General availability	26-Apr-2017	30-Nov-2020	TBA*
Note: * Dependent on next software release				

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual		Page 428 of 430

Appendix M. Certificates/Declaration of Conformity (DoC) Certificates

Table M-1 is a list of DoCs available for the ICCS equipment; refer to the following reference materials for actual documents.

HNL Directory: HNL-60125

Table M-1. List of DoCs for ACS

#	Document Name/Description
1	HNL-60126 06.00-41-4CO67 Altronix Declaration of Conformity_DoC.pdf
2	HNL-60126 06.00-41-4CO63 Genetec Declaration of Conformity_DoC.pdf
3	HNL-60126 06.00-41-4CO64- Genetec Declaration of Conformity_DoC_Additional1.pdf
4	HNL-60126 06.00-41-4CO65 Mercury Security Declaration of Conformity_DoC.pdf
5	HNL-60126 06.00-41-4CO66 HID Global Declaration of Conformity_DoC.pdf

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 429 of 430	

Appendix N. Reference Test Data

Table N-1 is a list of reference test data for the ACS equipment; refer to the following reference materials for actual documents.

HNL Directory: HNL-60876

Table N-1. Reference Test Data

#	Document Name/Description
1	3HR-79186-0876-XAZZA-06P01-HNL-60876 ACS-IDS SAT - Document
2	3HR-79186-0876-XBZZA-04P06-HNL-60876 ACS-IDS SAT - Appendix 01 - Test Cases
3	3HR-79101-FEAK-XAZZA-03-HNL-60172 Pre-shipment Inspection and Test Procedure - ACS IDS

END OF DOCUMENT

Document	HNL-62708	Revision	00.00
External Code	3HR-79XXX-XXXX-XXXX	Ext. Revision	
File Name	HNL-62708 00-o-COMMS SYSTEM – Security System: Access Control System (ACS) Operations Manual	Page 430 of 430	